114TH CONGRESS
2D SESSION

H. R. 1560

IN THE SENATE OF THE UNITED STATES

APRIL 27, 2015
Received

JULY 14, 2016
Read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, 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. TABLE OF CONTENTS.

The table of contents of this Act is as follows:

TITLE I—PROTECTING CYBER NETWORKS ACT

SEC. 101. SHORT TITLE.

This title may be cited as the ''Protecting Cyber Networks Act''.

SEC. 102. 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 Fed-

eral 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 under 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 infor-

mation 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 title, 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. 103. 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 title;

(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 purpose, operate a defensive measure that is operated on—

(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 a defensive measure that destroys, renders unusable or inaccessible (in whole or in part), or substantially harms 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 defensive 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 otherwise lawful sharing by a non-Federal entity of 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 title 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 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 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 104(d)(5)(A).

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure 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 title shall not create a right or benefit to similar information

by such non-Federal entity or any other non-Federal entity.

(f) SMALL BUSINESS PARTICIPATION.—

(1) ASSISTANCE.—The Administrator of the Small Business Administration shall provide assistance to small businesses and small financial institutions to monitor information and information systems, operate defensive measures, and share and receive cyber threat indicators and defensive measures under this section.

(2) REPORT.—Not later than 1 year after the date of the enactment of this title, the Administrator of the Small Business Administration shall submit to the President a report on the degree to which small businesses and small financial institutions are able to engage in cyber threat information sharing under this section. Such report shall include the recommendations of the Administrator for improving the ability of such businesses and institutions to engage in cyber threat information sharing and to use shared information to defend their networks.

(3) OUTREACH.—The Federal Government shall conduct outreach to small businesses and small financial institutions to encourage such businesses

and institutions to exercise their authority under this section.

SEC. 104. 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 102 of this title, 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 title, 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 title and the amendments made by this title.

(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 title, including guidelines to ensure that personal information of or information identifying specific persons is properly removed from information received, retained, used, or disseminated by a Federal entity in accordance with this title or the amendments made by this title;

(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 title, 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 102 of this title, 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 integrating 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 102 of this title, 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 title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with this title, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this title 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 title 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) 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 title 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 title 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, investigating, 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, investigating, prosecuting, 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 title 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 title 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. 105. 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 104(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 section unless such action is commenced not later than 2 years after the date on which the cause of action arises.

(d) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this section 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 title.

SEC. 106. 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 103(a) that is conducted in accordance with this title and the amendments made by this title.

(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 103(c), or a good faith failure to act based on such sharing or receipt, if such sharing or receipt is conducted

in accordance with this title and the amendments made by this title.

(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 title or the amendments made by this title; 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. 107. 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 102(a) and amended by section 104(a) of this title, is further amended—

(A) by redesignating subsection (c) (as redesignated by such section 104(a)) as subsection (d); and

(B) by inserting after subsection (b) (as inserted by such section 104(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 Con-

gress 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 pro-

vided 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) of such Act; or

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

''(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 1 year after the date of the enactment of this title.

(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 title.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this title 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 Inspec-

tor 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 title and the amendments made by this title.

(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.

(v) A review of the current procedures pertaining to the sharing of information, removal procedures for personal information or information identifying a specific person, and any incidents pertaining to the improper treatment of such 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 title or the amendments made by this title.

(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. 108. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this title, 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 to the national security and economy of the United States, 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 cybersecurity 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. 109. CONSTRUCTION AND PREEMPTION.

(a) PROHIBITION OF SURVEILLANCE.—Nothing in this title or the amendments made by this title 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 title or the amendments made by this title 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 title.

(c) WHISTLE BLOWER PROTECTIONS.—Nothing in this title or the amendments made by this title 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 title or the amendments made by this title 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 title or the amendments made by this title 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 title or the amendments made by this title 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 title or the amendments made by this title 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 title or the amendments made by this title 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 title or the amendments made by this title shall be construed to subject any non-Federal entity to liability for choosing not to engage in a voluntary activity authorized in this title and the amendments made by this title.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this title or the amendments made by this title 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 title or the amendments made by this title for any use other than permitted in this title or the amendments made by this title.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This title and the amendments made by this title 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 title or the amendments made by this title.

(2) STATE LAW ENFORCEMENT.—Nothing in this title or the amendments made by this title 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.

(3) STATE REGULATION OF UTILITIES.—Except as provided by section 103(d)(4)(B), nothing in this title or the amendments made by this title shall be construed to supersede any statute, regulation, or

other provision of law of a State or political subdivision of a State relating to the regulation of a private entity performing utility services, except to the extent such statute, regulation, or other provision of law restricts activity authorized under this title or the amendments made by this title.

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

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

(2) to establish any regulatory authority not specifically established under this title or the amendments made by this title; 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. 110. DEFINITIONS.

In this title:

(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 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).

SEC. 111. COMPTROLLER GENERAL REPORT ON REMOVAL OF PERSONAL IDENTIFYING INFORMATION.

(a) REPORT.—Not later than 3 years after the date of the enactment of this title, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators pursuant to section 104(b).

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 112. SUNSET.

This title and the amendments made by this title shall terminate on the date that is 7 years after the date of the enactment of this title.

TITLE II—NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT

SEC. 201. SHORT TITLE.

This title may be cited as the ''National Cybersecurity Protection Advancement Act of 2015''.

SEC. 202. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—Subsection (a) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(1) by amending paragraph (1) to read as follows:

''(1)(A) except as provided in subparagraph (B), the term 'cybersecurity risk' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, includ-

ing such related consequences caused by an act of terrorism;

''(B) such term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;''.

(2) by amending paragraph (2) to read as follows:

''(2) the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;''.

(3) in paragraph (3), by striking ''and'' at the end;

(4) in paragraph (4), by striking the period at the end and inserting ''; and''; and

(5) by adding at the end the following new paragraphs:

''(5) the term 'cyber threat indicator' means technical information that is necessary to describe or identify—

''(A) a method for probing, monitoring, maintaining, or establishing network awareness of an information system for the purpose of dis-

cerning technical vulnerabilities of such information system, if such method is known or reasonably suspected of being associated with a known or suspected cybersecurity risk, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity risk;

''(B) a method for defeating a technical or security control of an information system;

''(C) a technical vulnerability, including anomalous technical behavior that may become a 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 inadvertently enable the defeat of a technical or operational control;

''(E) 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 that is known or reasonably suspected of

being associated with a known or suspected cybersecurity risk;

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

''(G) any other attribute of a cybersecurity risk that cannot be used to identify specific persons reasonably believed to be unrelated to such cybersecurity risk, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination of subparagraphs (A) through (G);

''(6) the term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity risk or incident, or the purpose of identifying the source of a cybersecurity risk or incident;

''(7)(A) except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or

mitigates a known or suspected cybersecurity risk or incident, or any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control;

''(B) such term does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to—

''(i) the non-Federal entity, not including a State, local, or tribal government, operating such measure; or

''(ii) another Federal entity or non-Federal entity that is authorized to provide consent and has provided such consent to the non-Federal entity referred to in clause (i);

''(8) the term 'network awareness' means to scan, identify, acquire, monitor, log, or analyze information that is stored on, processed by, or transiting an information system;

''(9)(A) the term 'private entity' means a non-Federal entity that is an individual or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof;

''(B) such term includes a component of a State, local, or tribal government performing utility services or an entity performing utility services;

''(10) the term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentially, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system; and

''(11) the term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).''.

(b) AMENDMENT.—Subparagraph (B) of subsection (d)(1) of such second section 226 of the Homeland Security Act of 2002 is amended—

(1) in clause (i), by striking ''and local'' and inserting '', local, and tribal'';

(2) in clause (ii)—

(A) by inserting '', including information sharing and analysis centers'' before the semicolon; and

(B) by striking ''and'' at the end;

(3) in clause (iii), by inserting ''and'' after the semicolon at the end; and

(4) by adding at the end the following new clause:

''(iv) private entities;''.

SEC. 203. INFORMATION SHARING STRUCTURE AND PROCESSES.

The second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(1) in subsection (c)—

(A) in paragraph (1)—

(i) by striking ''a Federal civilian interface'' and inserting ''the lead Federal civilian interface''; and

(ii) by striking ''cybersecurity risks,'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(B) in paragraph (3), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(C) in paragraph (5)(A), by striking ''cybersecurity risks'' and inserting ''cyber threat

indicators, defensive measures, cybersecurity risks,'';

(D) in paragraph (6)—

(i) by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(ii) by striking ''and'' at the end;

(E) in paragraph (7)—

(i) in subparagraph (A), by striking ''and'' at the end;

(ii) in subparagraph (B), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following new subparagraph:

''(C) sharing cyber threat indicators and defensive measures;''; and

(F) by adding at the end the following new paragraphs:

''(8) engaging with international partners, in consultation with other appropriate agencies, to—

''(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

''(B) enhance the security and resilience of global cybersecurity;

''(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

''(10) promptly notifying the Secretary and the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of any significant violations of the policies and procedures specified in subsection (i)(6)(A);

''(11) promptly notifying non-Federal entities that have shared cyber threat indicators or defensive measures that are known or determined to be in error or in contravention of the requirements of this section; and

''(12) participating, as appropriate, in exercises run by the Department's National Exercise Program.'';

(2) in subsection (d)(1)—

(A) in subparagraph (D), by striking ''and'' at the end;

(B) by redesignating subparagraph (E) as subparagraph (J); and

(C) by inserting after subparagraph (D) the following new subparagraphs:

''(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center;

''(F) a United States Computer Emergency Readiness Team that coordinates information related to cybersecurity risks and incidents, proactively and collaboratively addresses cybersecurity risks and incidents to the United States, collaboratively responds to cybersecurity risks and incidents, provides technical assistance, upon request, to information system owners and operators, and shares cyber threat indicators, defensive measures, analysis, or information related to cybersecurity risks and incidents in a timely manner;

''(G) the Industrial Control System Cyber Emergency Response Team that—

''(i) coordinates with industrial control systems owners and operators;

"(ii) provides training, upon request, to Federal entities and non-Federal entities on industrial control systems cybersecurity;

"(iii) collaboratively addresses cybersecurity risks and incidents to industrial control systems;

"(iv) provides technical assistance, upon request, to Federal entities and non-Federal entities relating to industrial control systems cybersecurity;

"(v) shares cyber threat indicators, defensive measures, or information related to cybersecurity risks and incidents of industrial control systems in a timely fashion; and

"(vi) remains current on industrial control system innovation; industry adoption of new technologies, and industry best practices;

"(H) a National Coordinating Center for Communications that coordinates the protection, response, and recovery of emergency communications;

''(I) an entity that coordinates with small and medium-sized businesses; and'';

(3) in subsection (e)—

(A) in paragraph (1)—

(i) in subparagraph (A), by inserting ''cyber threat indicators, defensive measures, and'' before ''information'';

(ii) in subparagraph (B), by inserting ''cyber threat indicators, defensive measures, and'' before ''information'' the first place it appears;

(iii) in subparagraph (F), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(iv) in subparagraph (F), by striking ''and'' at the end;

(v) in subparagraph (G), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(vi) by adding at the end the following:

''(H) the Center ensures that it shares information relating to cybersecurity risks and in-

cidents with small and medium-sized businesses, as appropriate, and, to the extent practicable, make self-assessment tools available to such businesses to determine their levels of prevention of cybersecurity risks; and

''(I) the Center designates an agency contact for non-Federal entities;'';

(B) in paragraph (2)—

(i) by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(ii) by inserting ''or disclosure'' before the semicolon at the end; and

(C) in paragraph (3), by inserting before the period at the end the following: '', including by working with the Chief Privacy Officer appointed under section 222 to ensure that the Center follows the policies and procedures specified in subsection (i)(6)(A)''; and

(4) by adding at the end the following new subsections:

''(g) RAPID AUTOMATED SHARING.—

''(1) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection, in co-

ordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the timely sharing of cyber threat indicators and defensive measures to and from the Center and with each Federal agency designated as the 'Sector Specific Agency' for each critical infrastructure sector in accordance with subsection (h).

''(2) BIANNUAL REPORT.—The Under Secretary for Cybersecurity and Infrastructure Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a biannual report on the status and progress of the development of the capability described in paragraph (1). Such reports shall be required until such capability is fully implemented.

''(h) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of March 25, 2015, as the 'Sector Specific Agency' for each

critical infrastructure sector designated in the Department's National Infrastructure Protection Plan. If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for purposes of this section, the Secretary is deemed to be the head of such Sector Specific Agency and shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency, shall—

''(1) support the security and resilience actives of the relevant critical infrastructure sector in accordance with this section;

''(2) provide institutional knowledge, specialized expertise, and technical assistance upon request to the relevant critical infrastructure sector; and

''(3) support the timely sharing of cyber threat indicators and defensive measures with the relevant critical infrastructure sector with the Center in accordance with this section.

''(i) VOLUNTARY INFORMATION SHARING PROCEDURES.—

''(1) PROCEDURES.—

''(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and de-

fensive measures for cybersecurity purposes in accordance with this section. Nothing in this section may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has, after repeated notice, repeatedly violated the terms of this subsection.

''(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, if the Secretary determines that such is appropriate for national security.

''(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing rela-

tionship under this subsection may be characterized as an agreement described in this paragraph.

"(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

"(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, the Department shall negotiate a non-standard agreement, consistent with this section.

"(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of the enactment of this section, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect

under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

''(3) INFORMATION SHARING AUTHORIZATION.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), and notwithstanding any other provision of law, a non-Federal entity may, for cybersecurity purposes, share cyber threat indicators or defensive measures obtained on its own information system, or on an information system of another Federal entity or non-Federal entity, upon written consent of such other Federal entity or non-Federal entity or an authorized representative of such other Federal entity or non-Federal entity in accordance with this section with—

''(i) another non-Federal entity; or

''(ii) the Center, as provided in this section.

''(B) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another Federal entity or non-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 Federal entity or non-Federal entity.

''(C) REMOVAL OF INFORMATION UNRELATED TO CYBERSECURITY RISKS OR INCIDENTS.—Federal entities and non-Federal entities shall, prior to such sharing, take reasonable efforts to remove or exclude information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition.

''(D) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

''(i) limit or modify an existing information sharing relationship;

''(ii) prohibit a new information sharing relationship;

''(iii) require a new information sharing relationship between any non-Federal entity and a Federal entity;

''(iv) limit otherwise lawful activity; or

''(v) in any manner impact or modify procedures in existence as of the date of the enactment of this section for reporting known or suspected criminal activity to appropriate law enforcement authorities or for participating voluntarily or under legal requirement in an investigation.

''(E) COORDINATED VULNERABILITY DISCLOSURE.—The Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, shall develop, publish, and adhere to policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international standards in the information technology industry.

''(4) NETWORK AWARENESS AUTHORIZATION.—

''(A) IN GENERAL.—Notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government,

may, for cybersecurity purposes, conduct network awareness of—

"(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

"(ii) an information system of another non-Federal entity, upon written consent of such other non-Federal entity for conducting such network awareness to protect the rights or property of such other non-Federal entity;

"(iii) an information system of a Federal entity, upon written consent of an authorized representative of such Federal entity for conducting such network awareness to protect the rights or property of such Federal entity; or

"(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

"(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

"(i) authorize conducting network awareness of an information system, or the use of any information obtained through

such conducting of network awareness, other than as provided in this section; or

''(ii) limit otherwise lawful activity.

''(5) DEFENSIVE MEASURE AUTHORIZATION.—

''(A) IN GENERAL.—Except as provided in subparagraph (B) and notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government, may, for cybersecurity purposes, operate a defensive measure that is applied to—

''(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

''(ii) an information system of another non-Federal entity upon written consent of such other non-Federal entity for operation of such defensive measure to protect the rights or property of such other non-Federal entity;

''(iii) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of such Federal entity; or

"(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

"(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

"(i) authorize the use of a defensive measure other than as provided in this section; or

"(ii) limit otherwise lawful activity.

"(6) PRIVACY AND CIVIL LIBERTIES PROTECTIONS.—

"(A) POLICIES AND PROCEDURES.—

"(i) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, establish and annually review policies and procedures governing the receipt, retention, use, and disclosure of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents shared with the Center in accordance with this section. Such policies and procedures shall apply

only to the Department, consistent with the need to protect information systems from cybersecurity risks and incidents and mitigate cybersecurity risks and incidents in a timely manner, and shall—

"(I) be consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act of 1974' or the 'Privacy Act'), and subject to the Secretary's authority under subsection (a)(2) of section 222 of this Act;

"(II) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of cyber threat indicators and defensive measures associated with specific persons that is not necessary, for cybersecurity purposes, to protect a network or information system from cybersecurity risks or mitigate cybersecurity risks and incidents in a timely manner;

''(III) minimize any impact on privacy and civil liberties;

''(IV) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

''(V) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive, or that may be used to identify specific persons from unauthorized access or acquisition;

''(VI) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

"(VII) ensure all relevant constitutional, legal, and privacy protections are observed.

"(ii) SUBMISSION TO CONGRESS.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents described in clause (i) of subparagraph (A).

"(iii) PUBLIC NOTICE AND ACCESS.—The Under Secretary for Cybersecurity

and Infrastructure Protection, in consultation with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, and the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall ensure there is public notice of, and access to, the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents.

''(iv) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection when establishing policies and procedures to support privacy and civil liberties may consult with the National Institute of Standards and Technology.

''(B) IMPLEMENTATION.—The Chief Privacy Officer of the Department, on an ongoing basis, shall—

''(i) monitor the implementation of the policies and procedures governing the

sharing of cyber threat indicators and defensive measures established pursuant to clause (i) of subparagraph (A);

''(ii) regularly review and update privacy impact assessments, as appropriate, to ensure all relevant constitutional, legal, and privacy protections are being followed;

''(iii) work with the Under Secretary for Cybersecurity and Infrastructure Protection to carry out paragraphs (10) and (11) of subsection (c);

''(iv) annually submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a review of the effectiveness of such policies and procedures to protect privacy and civil liberties; and

''(v) ensure there are appropriate sanctions in place for officers, employees, or agents of the Department who intentionally or willfully conduct activities under this section in an unauthorized manner.

"(C) INSPECTOR GENERAL REPORT.—The Inspector General of the Department, in consultation with the Privacy and Civil Liberties Oversight Board and the Inspector General of each Federal agency that receives cyber threat indicators or defensive measures shared with the Center under this section, shall, not later than two years after the date of the enactment of this subsection and periodically thereafter submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing a review of the use of cybersecurity risk information shared with the Center, including the following:

"(i) A report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this section.

"(ii) Information on the use by the Center of such information for a purpose other than a cybersecurity purpose.

''(iii) A review of the type of information shared with the Center under this section.

''(iv) A review of the actions taken by the Center based on such information.

''(v) The appropriate metrics that exist to determine the impact, if any, on privacy and civil liberties as a result of the sharing of such information with the Center.

''(vi) A list of other Federal agencies receiving such information.

''(vii) A review of the sharing of such information within the Federal Government to identify inappropriate stove piping of such information.

''(viii) Any recommendations of the Inspector General of the Department for improvements or modifications to information sharing under this section.

''(D) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, in consultation with the Privacy and Civil Liberties Oversight Board,

the Inspector General of the Department, and the senior privacy and civil liberties officer of each Federal agency that receives cyber threat indicators and defensive measures shared with the Center under this section, shall biennially submit to the appropriate congressional committees a report assessing the privacy and civil liberties impact of the activities under this paragraph. Each such report shall include any recommendations the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat indicators and defensive measures under this section.

''(E) FORM.—Each report required under subparagraphs (C) and (D) shall be submitted in unclassified form, but may include a classified annex.

''(7) USES AND PROTECTION OF INFORMATION.—

''(A) NON-FEDERAL ENTITIES.—A non-Federal entity, not including a State, local, or tribal government, that shares cyber threat in-

dicators or defensive measures through the Center or otherwise under this section—

"(i) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

"(ii) shall, prior to such sharing, take reasonable efforts to remove or exclude information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

"(iii) shall comply with appropriate restrictions that a Federal entity or non-Federal entity places on the subsequent disclosure or retention of cyber threat indicators and defensive measures that it discloses to other Federal entities or non-Federal entities;

''(iv) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

''(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

''(vi) may not use such information to gain an unfair competitive advantage to the detriment of any non-Federal entity.

''(B) FEDERAL ENTITIES.—

''(i) USES OF INFORMATION.—A Federal entity that receives cyber threat indicators or defensive measures shared through the Center or otherwise under this section from another Federal entity or a non-Federal entity—

''(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

''(II) shall, prior to such sharing, take reasonable efforts to remove or exclude information that can be used

to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

''(III) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

''(IV) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

''(V) may not use such cyber threat indicators or defensive measures to engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information, except for purposes authorized in this section.

"(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

"(I) are exempt from disclosure under section 552 of title 5, United States Code, and withheld, without discretion, from the public under subsection (b)(3)(B) of such section;

"(II) may not be used by the Federal Government for regulatory purposes;

"(III) may not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection;

"(IV) shall be considered the commercial, financial, and proprietary information of the non-Federal entity referred to in clause (i) when so designated by such non-Federal entity; and

"(V) may not be subject to a rule of any Federal entity or any judicial doctrine regarding ex parte commu-

nications with a decisionmaking official.

''(C) STATE, LOCAL, OR TRIBAL GOVERNMENT.—

''(i) USES OF INFORMATION.—A State, local, or tribal government that receives cyber threat indicators or defensive measures from the Center from a Federal entity or a non-Federal entity—

''(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

''(II) shall, prior to such sharing, take reasonable efforts to remove or exclude information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

''(III) shall consider such information the commercial, financial, and proprietary information of such Federal entity or non-Federal entity if so designated by such Federal entity or non-Federal entity;

''(IV) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures; and

''(V) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures.

''(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

''(I) shall be exempt from disclosure under any State, local, or tribal law or regulation that requires public disclosure of information or records by a public or quasi-public entity; and

''(II) may not be used by any State, local, or tribal government to

regulate a lawful activity of a non-Federal entity.

''(8) LIABILITY EXEMPTIONS.—

''(A) NETWORK AWARENESS.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, conducts network awareness under paragraph (4), if such network awareness is conducted in accordance with such paragraph and this section.

''(B) INFORMATION SHARING.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, shares cyber threat indicators or defensive measures under paragraph (3), or in good faith fails to act based on such sharing, if such sharing is conducted in accordance with such paragraph and this section.

''(C) WILLFUL MISCONDUCT.—

''(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

''(I) require dismissal of a cause of action against a non-Federal entity

that has engaged in willful misconduct in the course of conducting activities authorized by this section; or

"(II) undermine or limit the availability of otherwise applicable common law or statutory defenses.

"(ii) PROOF OF WILLFUL MISCONDUCT.—In any action claiming that subparagraph (A) or (B) does not apply due to willful misconduct described in clause (i), 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.

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

"(I) intentionally to achieve a wrongful purpose;

"(II) knowingly without legal or factual justification; and

"(III) 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.

"(D) EXCLUSION.—The term 'non-Federal entity' as used in this paragraph shall not include a State, local, or tribal government.

"(9) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE USE AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

"(A) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates the restrictions specified in paragraph (3), (6), or (7)(B) on the use and protection of voluntarily shared cyber threat indicators or defensive measures, or any other provision of this section, the Federal Government shall be liable to a person injured by such violation in an amount equal to the sum of—

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

"(ii) reasonable attorney fees as determined by the court and other litigation

costs reasonably occurred in any case under this subsection in which the complainant has substantially prevailed.

''(B) VENUE.—An action to enforce liability under this subsection may be brought in the district court of the United States in—

''(i) the district in which the complainant resides;

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

''(iii) the district in which the department or agency of the Federal Government that disclosed the information is located; or

''(iv) 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 on which the cause of action arises.

''(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 of any restric-

tion specified in paragraph (3), (6), or 7(B) or any other provision of this section.

''(10) ANTI-TRUST EXEMPTION.—

''(A) IN GENERAL.—Except as provided in subparagraph (C), it shall not be considered a violation of any provision of antitrust laws for two or more non-Federal entities to share a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity risk or incident, for cybersecurity purposes under this Act.

''(B) APPLICABILITY.—Subparagraph (A) shall apply only to information that is shared or assistance that is provided in order to assist with—

''(i) facilitating the prevention, investigation, or mitigation of a cybersecurity risk or incident to an information system or information that is stored on, processed by, or transiting an information system; or

''(ii) communicating or disclosing a cyber threat indicator or defensive measure to help prevent, investigate, or mitigate the effect of a cybersecurity risk or incident to

an information system or information that is stored on, processed by, or transiting an information system.

"(11) CONSTRUCTION AND PREEMPTION.—

"(A) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section may be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity or participating voluntarily or under legal requirement in an investigation, by a non-Federal to any other non-Federal entity or Federal entity under this section.

"(B) WHISTLE BLOWER PROTECTIONS.—Nothing in this section may 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), section 1104 of the

National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

''(C) RELATIONSHIP TO OTHER LAWS.—Nothing in this section may be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to a Federal entity.

''(D) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this section may be construed to—

''(i) 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

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

''(E) ANTI-TASKING RESTRICTION.—Nothing in this section may be construed to permit a Federal entity to—

"(i) require a non-Federal entity to provide information to a Federal entity;

"(ii) condition the sharing of cyber threat indicators or defensive measures with a non-Federal entity on such non-Federal entity's provision of cyber threat indicators or defensive measures to a Federal entity; or

"(iii) condition the award of any Federal grant, contract, or purchase on the sharing of cyber threat indicators or defensive measures with a Federal entity.

"(F) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section may be construed to subject any non-Federal entity to liability for choosing to not engage in the voluntary activities authorized under this section.

"(G) USE AND RETENTION OF INFORMATION.—Nothing in this section may 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 section for any use other than permitted in this section.

''(H) VOLUNTARY SHARING.—Nothing in this section may be construed to restrict or condition a non-Federal entity from sharing, for cybersecurity purposes, cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with any other non-Federal entity, and nothing in this section may be construed as requiring any non-Federal entity to share cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with the Center.

''(I) PROHIBITED CONDUCT.—Nothing in this section may be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

''(J) FEDERAL PREEMPTION.—This section supersedes 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 section.

''(j) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the

Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

''(k) ADDITIONAL RESPONSIBILITIES.—The Secretary shall build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems.

''(l) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of the enactment of this subsection and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

''(m) OUTREACH.—Not later than 60 days after the date of the enactment of this subsection, the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, shall—

''(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

''(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.''.

SEC. 204. INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.

Section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131) is amended—

(1) in paragraph (5)—

(A) in subparagraph (A)—

(i) by inserting ''and information related to cybersecurity risks and incidents and'' after ''critical infrastructure information''; and

(ii) by striking ''related to critical infrastructure'' and inserting ''related to cybersecurity risks, incidents, critical infrastructure, and'';

(B) in subparagraph (B)—

(i) by striking ''disclosing critical infrastructure information'' and inserting ''disclosing cybersecurity risks, incidents, and critical infrastructure information''; and

(ii) by striking ''related to critical infrastructure or'' and inserting ''related to cybersecurity risks, incidents, critical infrastructure, or'' and

(C) in subparagraph (C), by striking ''disseminating critical infrastructure information''

and inserting ''disseminating cybersecurity risks, incidents, and critical infrastructure information''; and

(2) by adding at the end the following new paragraph:

''(8) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given such terms in the second section 226 (relating to the National Cybersecurity and Communications Integration Center).''.

SEC. 205. STREAMLINING OF DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE PROTECTION ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this title, be known and designated as the ''Cybersecurity and Infrastructure Protection''. Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection of the Department.

(b) SENIOR LEADERSHIP OF CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended—

(A) in paragraph (1)—

(i) by amending subparagraph (H) to read as follows:

''(H) An Under Secretary for Cybersecurity and Infrastructure Protection.''; and

(ii) by adding at the end the following new subparagraphs:

''(K) A Deputy Under Secretary for Cybersecurity.

''(L) A Deputy Under Secretary for Infrastructure Protection.''; and

(B) by adding at the end the following new paragraph:

''(3) DEPUTY UNDER SECRETARIES.—The Deputy Under Secretaries referred to in subparagraphs (K) and (L) of paragraph (1) shall be appointed by the President without the advice and consent of the Senate.''.

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred in subparagraphs (H), (K), and (L) of paragraph (1) of section 103(a) the Homeland Security Act of 2002 (as amended and added by paragraph (1) of this subsection) as of the date of the enactment of this title may continue to hold such positions.

(c) REPORT.—Not later than 90 days after the date of the enactment of this title, the Under Secretary for Cybersecurity and Infrastructure Protection of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of becoming an operational component, including an analysis of alternatives, and if a determination is rendered that becoming an operational component is the best option for achieving the mission of Cybersecurity and Infrastructure Protection, a legislative proposal and implementation plan for becoming such an operational component. Such report shall also include plans to more effectively carry out the cybersecurity mission of Cybersecurity and Infrastructure Protection, including expediting information sharing agreements.

SEC. 206. CYBER INCIDENT RESPONSE PLANS.

(a) IN GENERAL.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 149) is amended—

(1) in the heading, by striking ''**PLAN**'' and inserting ''**PLANS**'';

(2) by striking ''The Under Secretary appointed under section 103(a)(1)(H) shall'' and inserting the following:

''(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall''; and

(3) by adding at the end the following new subsection:

''(b) UPDATES TO THE CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (a), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by amending the item relating to section 227 to read as follows:

''Sec. 227. Cyber incident response plans.''.

SEC. 207. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS; CYBERSECURITY AWARENESS CAMPAIGN.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new sections:

"SEC. 230. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS.

"The National Cybersecurity and Communications Integration Center, in coordination with the Office of Emergency Communications of the Department, shall assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

"SEC. 231. CYBERSECURITY AWARENESS CAMPAIGN.

"(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall develop and implement an ongoing and comprehensive cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks. Such campaign shall, at a minimum, publish and disseminate, on an ongoing basis, the following:

"(1) Public service announcements targeted at improving awareness among State, local, and tribal

governments, the private sector, academia, and stakeholders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans.

''(2) Vendor and technology-neutral voluntary best practices information.

''(b) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection shall consult with a wide range of stakeholders in government, industry, academia, and the non-profit community in carrying out this section.

''SEC. 232. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

''(a) IN GENERAL.—The Secretary may establish a consortium to be known as the 'National Cybersecurity Preparedness Consortium' (in this section referred to as the 'Consortium').

''(b) FUNCTIONS.—The Consortium may—

''(1) provide training to State and local first responders and officials specifically for preparing and responding to cyber attacks;

''(2) develop and update a curriculum utilizing the National Protection and Programs Directorate of the Department sponsored Community Cyber Se-

curity Maturity Model (CCSMM) for State and local first responders and officials;

''(3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response;

''(4) conduct cybersecurity training and simulation exercises to defend from and respond to cyberattacks;

''(5) coordinate with the National Cybersecurity and Communications Integration Center to help States and communities develop cybersecurity information sharing programs; and

''(6) coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity emergency responses into existing State and local emergency management functions.

''(c) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that develop, update, and deliver cybersecurity training in support of homeland security. Members shall have prior experience conducting cybersecurity training and exercises for State and local entities.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to

cybersecurity recruitment and retention) the following new items:

"Sec. 230. Security and resiliency of public safety communications.
"Sec. 231. Cybersecurity awareness campaign.
"Sec. 232. National Cybersecurity Preparedness Consortium.".

SEC. 208. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

"SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Secretary, acting through the Under Secretary for Science and Technology, shall submit to Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Such plan shall be updated and submitted to Congress every two years.

"(b) CONTENTS OF PLAN.—The strategic plan, including biennial updates, required under subsection (a) shall include the following:

''(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following:

''(A) Consultation with stakeholders, including critical infrastructure Sector Coordinating Councils.

''(B) Performance by the Department of a risk and gap analysis that considers information received in such consultations.

''(2) A set of critical infrastructure security technology needs that—

''(A) is prioritized based on the risks and gaps identified under paragraph (1);

''(B) emphasizes research and development of technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure technology; and

''(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

''(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

''(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection, including a consideration of opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

''(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan required under subsection (a).

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate with the Under Secretary for the National Protection and Programs Directorate.

''(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

''(1) critical infrastructure Sector Coordinating Councils;

''(2) to the extent practicable, subject matter experts on critical infrastructure protection from

universities, colleges, national laboratories, and private industry;

''(3) the heads of other relevant Federal departments and agencies that conduct research and development relating to critical infrastructure protection; and

''(4) State, local, and tribal governments, as appropriate.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 317 the following new item:

''Sec. 318. Research and development strategy for critical infrastructure protection.''.

SEC. 209. REPORT ON REDUCING CYBERSECURITY RISKS IN DHS DATA CENTERS.

Not later than 1 year after the date of the enactment of this title, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of the Department of Homeland Security creating an environment for the reduction in cybersecurity risks in Department data centers, including by increasing compartmentalization between systems, and providing a mix of security controls between such compartments.

SEC. 210. ASSESSMENT.

Not later than 2 years after the date of the enactment of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains an assessment of the implementation by the Secretary of Homeland Security of this title and the amendments made by this title and, to the extent practicable, findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents at the National Cybersecurity and Communications Integration Center and throughout the United States.

SEC. 211. CONSULTATION.

The Under Secretary for Cybersecurity and Infrastructure Protection shall produce a report on the feasibility of creating a risk-informed prioritization plan should multiple critical infrastructures experience cyber incidents simultaneously.

SEC. 212. TECHNICAL ASSISTANCE.

The Inspector General of the Department of Homeland Security shall review the operations of the United States Computer Emergency Readiness Team (US–CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) to assess the capacity

to provide technical assistance to non-Federal entities and to adequately respond to potential increases in requests for technical assistance.

SEC. 213. PROHIBITION ON NEW REGULATORY AUTHORITY.

Nothing in this title or the amendments made by this title may be construed to grant the Secretary of Homeland Security any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of the enactment of this title.

SEC. 214. SUNSET.

Any requirements for reports required by this title or the amendments made by this title shall terminate on the date that is 7 years after the date of the entitlement of this title.

SEC. 215. PROHIBITION ON NEW FUNDING.

No funds are authorized to be appropriated to carry out this title and the amendments made by this title. This title and such amendments shall be carried out using amounts appropriated or otherwise made available for such purposes.

SEC. 216. PROTECTION OF FEDERAL INFORMATION SYSTEMS.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

"SEC. 233. AVAILABLE PROTECTION OF FEDERAL INFORMATION SYSTEMS.

''(a) IN GENERAL.—The Secretary shall deploy and operate, to make available for use by any Federal agency, with or without reimbursement, capabilities to protect Federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks (as such term is defined in the second section 226) involving Federal agency information or information systems.

''(b) ACTIVITIES.—In carrying out this section, the Secretary may—

''(1) access, and Federal agency heads may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information traveling to or from or stored on a Federal agency information system, regardless of from where the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or pre-

vent Federal agency heads from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

"(2) enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (a); and

"(3) retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect Federal agency information and information systems from cybersecurity risks, or, with the approval of the Attorney General and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to—

"(A) a violation of section 1030 of title 18, United States Code;

"(B) an imminent threat of death or serious bodily harm;

"(C) a serious threat to a minor, including sexual exploitation or threats to physical safety; or

"(D) an attempt, or conspiracy, to commit an offense described in any of subparagraphs (A) through (C).

"(c) CONDITIONS.—Contracts or other agreements under subsection (b)(2) shall include appropriate provisions barring—

"(1) the disclosure of information to any entity other than the Department or the Federal agency disclosing information in accordance with subsection (b)(1) that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk; and

"(2) the use of any information to which such private entity gains access in accordance with this section for any purpose other than to protect Federal agency information and information systems against cybersecurity risks or to administer any such contract or other agreement.

"(d) LIMITATION.—No cause of action shall lie against a private entity for assistance provided to the Secretary in accordance with this section and a contract or agreement under subsection (b)(2).".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to

cybersecurity recruitment and retention) the following new item:

''Sec. 233. Available protection of Federal information systems.''.

SEC. 217. SUNSET.

This title and the amendments made by this title shall terminate on the date that is 7 years after the date of the enactment of this title.

SEC. 218. REPORT ON CYBERSECURITY VULNERABILITIES OF UNITED STATES PORTS.

Not later than 180 days after the date of the enactment of this title, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science and Transportation of the Senate a report on cybersecurity vulnerabilities for the ten United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities.

SEC. 219. REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE.

The Secretary of Homeland Security may consult with sector specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security of the House of Representatives and the Committee

on Homeland Security and Governmental Affairs of the Senate a report on how best to align federally funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure, including—

(1) promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;

(2) enhancing modeling capabilities to determine potential impacts on critical infrastructure of incidents or threat scenarios, and cascading effects on other sectors; and

(3) facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen cybersecurity and resilience.

SEC. 220. GAO REPORT ON IMPACT PRIVACY AND CIVIL LIBERTIES.

Not later than 60 months after the date of the enactment of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the

Senate an assessment on the impact on privacy and civil liberties limited to the work of the National Cybersecurity and Communications Integration Center.

Passed the House of Representatives April 22, 2015.

Attest: KAREN L. HAAS,

Clerk.