111TH CONGRESS
2D SESSION

S. 3538

To improve the cyber security of the United States and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 24, 2010

Mr. BOND (for himself and Mr. HATCH) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To improve the cyber security of the United States and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cyber Infrastructure Protection Act of 2010''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Energy and Natural Resources, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016 of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c).

(3) CYBER SECURITY ACTIVITIES.—The term ''cyber security activities'' means a class or collection of similar cyber security operations of a Federal agency that involves personally identifiable data that is—

(A) screened by a cyber security system outside of the Federal agency that was the intended recipient of the personally identifiable data;

(B) transferred, for the purpose of cyber security, outside such Federal agency; or

(C) transferred, for the purpose of cyber security, to an element of the intelligence community.

(4) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United States Code.

(5) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(6) LOCAL GOVERNMENT.—The term ''local government'' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(7) NATIONAL CYBER SECURITY PROGRAM.—The term ''National Cyber Security Program'' means the programs, projects, and activities of the Federal Government to protect and defend Federal Government information networks and to facilitate the protection and defense of United States information networks.

(8) NETWORK.—The term ''network'' has the meaning given that term by section 4(5) of the High-Performance Computing Act of 1991 (15 U.S.C. 5503(5)).

(9) STATE.—The term ''State'' means—

(A) a State;

(B) the District of Columbia;

(C) the Commonwealth of Puerto Rico; and

(D) any other territory or possession of the United States.

TITLE I—NATIONAL CYBER CENTER

SEC. 101. DIRECTOR DEFINED.

In this title, except as otherwise specifically provided, the term ''Director'' means the Director of the National Cyber Center appointed under section 103.

SEC. 102. ESTABLISHMENT OF THE NATIONAL CYBER CENTER.

(a) IN GENERAL.—There is within the Department of Defense a National Cyber Center.

(b) ADMINISTRATIVE AND LOGISTICAL SUPPORT.—Except as otherwise specifically provided in this Act, the Secretary of Defense shall provide only administrative and

logistical support for the daily operation of the National Cyber Center.

SEC. 103. DIRECTOR OF THE NATIONAL CYBER CENTER.

(a) IN GENERAL.—The head of the National Cyber Center is the Director of the National Cyber Center, who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) TERM AND CONDITIONS OF APPOINTMENT.—A Director shall serve for a term not to exceed five years and during such term may not simultaneously serve in any other capacity in the Executive branch.

(c) REPORTING AND PLACEMENT.—

(1) REPORTING.—The Director shall report directly to the President.

(2) PLACEMENT.—The position of the Director shall not be located within the Executive Office of the President.

(d) DUTIES OF THE DIRECTOR.—The Director shall—

(1) coordinate Federal Government defensive operations, intelligence collection and analysis, and activities to protect and defend Federal Government information networks;

(2) act as the principal adviser to the President, the National Security Council, and to the

heads of Federal agencies on matters relating to the protection and defense of Federal Government information networks;

(3) coordinate, and ensure the adequacy of, the National Cyber Security Program budgets for Federal agencies;

(4) maintain and disperse funds from the National Cyber Defense Contingency Fund in accordance with section 108;

(5) ensure appropriate coordination within the Federal Government for the implementation of any cyber security activities conducted by a Federal agency;

(6) ensure appropriate coordination within the Federal Government for the conduct of any operations, strategies, and intelligence collection and analysis relating to the protection and defense of Federal Government information networks;

(7) provide recommendations, on an ongoing basis, to Federal agencies, private sector entities, and public and private sector entities operating critical infrastructure for procedures to be implemented in the event of an imminent cyber attack that will protect critical infrastructure by mitigating network vulnerabilities;

(8) provide assistance to, and cooperate with, the Cyber Defense Alliance established under section 202, including the development of partnerships with public and private sector entities, and academic institutions that encourage cooperation, research, development, and cyber security education and training;

(9) develop plans and policies for the security of Federal Government information networks to be implemented by the appropriate Federal agency;

(10) participate in the process to develop reliability standards pursuant to section 215 of the Federal Power Act (16 U.S.C. 824o);

(11) develop plans and policies for the sharing of cyber threat-related information among appropriate Federal agencies, and to the extent consistent with the protection of national security sources and methods, with State, tribal, and local government departments, agencies, and entities, and public and private sector entities that operate critical infrastructure;

(12) develop policies and procedures to ensure the continuity of Federal Government operations in the event of a national cyber crisis; and

(13) perform such other functions as may be directed by the President.

SEC. 104. MISSIONS OF THE NATIONAL CYBER CENTER.

(a) IN GENERAL.—The National Cyber Center shall—

(1) serve as the primary organization for coordinating Federal Government defensive operations, intelligence collection and analysis, and activities to protect and defend Federal Government information networks;

(2) develop policies and procedures for implementation across the Federal Government on matters relating to the protection and defense of Federal Government information networks;

(3) provide a process for resolving conflicts among Federal agencies relating to the implementation of cyber security activities or the conduct of operations, strategies, and intelligence collection and analysis relating to the protection and defense of Federal Government information networks;

(4) assign roles and responsibilities to Federal agencies, as appropriate, for the protection and defense of Federal Government information networks that are consistent with applicable law; and

(5) ensure that, as appropriate, Federal agencies have access to, and receive, information, including appropriate private sector information, regarding cyber threats to Federal Government information networks.

(b) ACCESS TO INTELLIGENCE.—The Director shall have access to all intelligence relating to cyber security collected by any Federal agency—

(1) except as otherwise provided by law;

(2) unless otherwise directed by the President; or

(3) unless the Attorney General and the Director agree on guidelines to limit such access.

SEC. 105. COMPOSITION OF NATIONAL CYBER CENTER.

(a) INTEGRATION OF RESOURCES.—Not later than 90 days after the date of the confirmation of the initial Director, the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation shall, in consultation with the Director, collocate and integrate within the National Cyber Center such elements, offices, task forces, and other components of the Department of Defense, the Department of Homeland Security, the intelligence community, and the Federal Bureau of In-

vestigation that are necessary to carry out the missions of the National Cyber Center.

(b) PARTICIPATION OF FEDERAL AGENCIES.—Any Federal agency not referred to in subsection (a) may participate in the National Cyber Center if the head of such Federal agency and the Director agree on the level and type of such participation.

(c) RECOMMENDATIONS FOR CONSOLIDATION.—In order to reduce duplication of Federal Government efforts, the Director may recommend that the President transfer to, and consolidate within, the National Cyber Center activities that relate to the protection and defense of Federal Government information networks.

(d) INTEGRATION OF INFORMATION NETWORKS.—The Director shall, in coordination with the appropriate head of a Federal agency, oversee the integration within the National Cyber Center of information relating to the protection and defense of Federal Government information networks, including to the extent necessary and consistent with the protection of sources and methods, databases containing such information.

SEC. 106. NATIONAL CYBER CENTER OFFICIALS.

(a) DEPUTY DIRECTOR.—

(1) IN GENERAL.—There is a Deputy Director of the National Cyber Center who shall be appointed by the Director.

(2) APPOINTMENT CRITERIA.—An individual appointed Deputy Director of the National Cyber Center shall have extensive cyber security and management expertise.

(3) DUTIES.—The Deputy Director shall—

(A) assist the Director in carrying out the duties and responsibilities of the Director; and

(B) act for, and exercise the powers of, the Director during the absence or disability of the Director or during a vacancy in the position of Director.

(b) GENERAL COUNSEL.—

(1) IN GENERAL.—There is a General Counsel of the National Cyber Center who shall be appointed by the Director.

(2) DUTIES.—The General Counsel is the chief legal officer of the National Cyber Center and shall perform such functions as the Director may prescribe.

(c) OTHER OFFICIALS.—The Director may designate such other officials in the National Cyber Center as the Director determines appropriate.

(d) STAFF.—To assist the Director in fulfilling the duties and responsibilities of the Director, the Director shall employ and utilize a professional staff having expertise in matters relating to the mission of the National Cyber Center, and may establish permanent positions and appropriate rates of pay with respect to such staff.

SEC. 107. NATIONAL CYBER SECURITY PROGRAM BUDGET.

(a) SUBMISSION OF CYBER BUDGET REQUEST TO THE DIRECTOR.—For each fiscal year, the head of each Federal agency with responsibilities for matters relating to the protection and defense of Federal Government information networks shall transmit to the Director a copy of the proposed National Cyber Security Program budget request of the agency prior to the submission of such proposed budget request to the Office of Management and Budget in the preparation of the budget of the President submitted to Congress under section 1105(a) of title 31, United States Code.

(b) REVIEW AND CERTIFICATION OF BUDGET REQUESTS AND BUDGET SUBMISSIONS.—

(1) IN GENERAL.—The Director shall review each budget request submitted to the Director under subsection (a).

(2) REVIEW OF BUDGET REQUESTS.—

(A) INADEQUATE REQUESTS.—If the Director concludes that a budget request submitted under subsection (a) for a Federal agency is inadequate to accomplish the protection and defense of Federal Government information networks, or to facilitate the protection and defense of United States information networks, with respect to such Federal agency for the year for which the request is submitted, the Director shall submit to the head of such Federal agency a written description of funding levels and specific initiatives that would, in the determination of the Director, make the request adequate to accomplish the protection and defense of such information networks.

(B) ADEQUATE REQUESTS.—If the Director concludes that a budget request submitted under subsection (a) for a Federal agency is adequate to accomplish the protection and defense of Federal Government information networks, or to facilitate the protection and defense of United States information networks, with respect to such Federal agency for the year for which the request is submitted, the Director shall submit to the head of such Federal

agency a written statement confirming the adequacy of the request.

(C) RECORD.—The Director shall maintain a record of each description submitted under subparagraph (A) and each statement submitted under subparagraph (B).

(3) AGENCY RESPONSE.—

(A) IN GENERAL.—The head of a Federal agency that receives a description under paragraph (2)(A) shall include the funding levels and initiatives described by the Director in the National Cyber Security Program budget submission for such Federal agency to the Office of Management and Budget.

(B) IMPACT STATEMENT.—If the head of a Federal agency alters the National Cyber Security Program budget submission of such agency based on a description received under paragraph (2)(A), such head shall include as an appendix to the budget submitted to the Office of Management and Budget for such agency an impact statement that summarizes—

(i) the changes made to the budget based on such description; and

(ii) the impact of such changes on the ability of such agency to perform its other responsibilities, including any impact on specific missions or programs of such agency.

(4) CONGRESSIONAL NOTIFICATION.—The head of a Federal agency shall submit to Congress a copy of any impact statement prepared under paragraph (3)(B) at the time the National Cyber Security Program budget for such agency is submitted to Congress under section 1105(a) of title 31, United States Code.

(5) CERTIFICATION OF NATIONAL CYBER SECURITY PROGRAM BUDGET SUBMISSIONS.—

(A) IN GENERAL.—At the time the head of a Federal agency submits a National Cyber Security Program budget request for such agency for a fiscal year to the Office of Management and Budget, such head shall submit a copy of the National Cyber Security Program budget request to the Director.

(B) DECERTIFICATION.—

(i) IN GENERAL.—The Director shall review each National Cyber Security Pro-

gram budget request submitted under subparagraph (A).

(ii) BUDGET DECERTIFICATION.—If, based on the review under clause (i), the Director concludes that such budget request does not include the funding levels and specific initiatives that would, in the determination of the Director, make the request adequate to accomplish the protection and defense of Federal Government information networks, or to facilitate the protection and defense of United States information networks, the Director may issue a written decertification of such Federal agency's budget.

(iii) SUBMISSION TO CONGRESS.—In the case of a decertification of a budget request issued under clause (ii), the Director shall submit to Congress a copy of—

(I) such National Cyber Security Program budget request;

(II) such decertification; and

(III) the description made for the budget request under paragraph (2)(B).

(c) CONSOLIDATED NATIONAL CYBER SECURITY PROGRAM BUDGET PROPOSAL.—For each fiscal year, following the transmission of proposed National Cyber Security Program budget requests for Federal agencies to the Director under subsection (a), the Director shall, in consultation with the head of such Federal agencies—

(1) develop a consolidated National Cyber Security Program budget proposal;

(2) submit the consolidated budget proposal to the President; and

(3) after making the submission required by paragraph (2), submit the consolidated budget proposal to Congress.

SEC. 108. NATIONAL CYBER DEFENSE CONTINGENCY FUND.

(a) ESTABLISHMENT OF FUND.—There is established within the National Cyber Security Program Budget a fund to be known as the ''National Cyber Defense Contingency Fund,'' which shall consist of amounts appropriated to the Fund for the purpose of providing financial assistance and technical and operational support in the event of a significant cyber incident.

(b) ADMINISTRATION.—The Director shall be responsible for the administration and management of the amounts in the National Cyber Defense Contingency Fund.

(c) USE.—In response to a significant cyber incident involving Federal Government or United States information networks, the Director may distribute amounts from the National Cyber Defense Contingency Fund to appropriate Federal agencies.

(d) NOTIFICATION.—Prior to distributing amounts under this section, the Director shall notify the appropriate congressional committees.

(e) SIGNIFICANT CYBER INCIDENT DEFINED.—In this section, the term ''significant cyber incident'' means a malicious act, suspicious event, or accident that—

(1) causes a disruption of Federal Government or United States information networks;

(2) affects one or more Federal agencies or public or private sector entities operating critical infrastructure;

(3) affects more than one State or a substantial number of residents in one or more States; and

(4) results in a substantial likelihood of harm or financial loss to the United States or its citizens.

SEC. 109. PROGRAM BUDGET SUBMISSION.

(a) SUBMISSION.—Section 1105(a) of title 31, United States Code, is amended by adding at the end the following:

''(38) a separate statement of the combined and individual amounts of appropriations requested for the National Cyber Security Program, including a separate statement of the amounts of appropriations requested by the Secretary of Defense for the operation and activities of the National Cyber Center and a separate statement of the amounts of appropriations requested by the Secretary of Energy for the operation and activities of the Cyber Defense Alliance.''.

(b) TECHNICAL AMENDMENTS.—Section 1105(a) of title 31, United States Code, as amended by subsection (a), is further amended—

(1) by redesignating the paragraph (33) added by section 889 of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2250) as paragraph (35);

(2) by redesignating the paragraph (35) added by section 203 of the Emergency Economic Stabilization Act of 2008 (division A of Public Law 110–343; 122 Stat. 3765) as paragraph (36); and

(3) by redesignating the paragraph (36) added by section 2 of the Veterans Health Care Budget Reform and Transparency Act of 2009 (Public Law 111–81; 123 Stat. 2137) as paragraph (37).

SEC. 110. CONSTRUCTION.

Except as otherwise specifically provided, nothing in this title shall be construed as terminating, altering, or otherwise affecting any authority of the head of a Federal agency collocated within or otherwise participating in the National Cyber Center.

SEC. 111. CONGRESSIONAL OVERSIGHT.

The Director shall keep the appropriate congressional committees fully and currently informed of the significant activities of the National Cyber Center relating to ensuring the security of Federal Government information networks.

TITLE II—CYBER DEFENSE ALLIANCE

SEC. 201. DEFINITIONS.

In this title:

(1) BOARD.—The term ''Board'' means the Board of Directors of the Cyber Defense Alliance established pursuant to section 204(a).

(2) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given that term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

SEC. 202. CYBER DEFENSE ALLIANCE.

(a) CHARTER.—There is within a National Laboratory a public and private partnership for sharing cyber

threat information and exchanging technical assistance, advice, and support to be known as the Cyber Defense Alliance.

(b) ESTABLISHMENT.—The Secretary of Energy, in coordination with the Director of the National Cyber Center, the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, shall determine the appropriate location for, and establish, the Cyber Defense Alliance.

(c) CRITERIA.—The criteria to be used in selecting a National Laboratory under subsection (a) shall include the following:

(1) Whether the National Laboratory has received recognition from members of the intelligence community, the Secretary of Homeland Security, or the Secretary of Defense for its cyber capabilities.

(2) Whether the National Laboratory has demonstrated the ability to address cyber-related issues involving varying levels of classified information.

(3) Whether the National Laboratory has demonstrated the capability to develop cooperative relationships with the private sector on cyber-related issues.

(d) PARTNERSHIP.—If the Secretary of Energy, the Director of the National Cyber Center, the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation determine that the missions and activities of the Cyber Defense Alliance may only be accomplished through a partnership of two or more National Laboratories acting jointly to support the Alliance, then the Alliance may be established and located within such National Laboratories.

SEC. 203. MISSION AND ACTIVITIES.

The Cyber Defense Alliance shall—

(1) facilitate the exchange of ideas and technical assistance and support related to the security of public, private, and critical infrastructure information networks;

(2) promote research and development, including the advancement of private funding for research and development, related to ensuring the security of public, private, and critical infrastructure information networks;

(3) serve as a national clearinghouse for the exchange of cyber threat information for the benefit of the private sector, educational institutions, State, tribal, and local governments, public and private sec-

tor entities operating critical infrastructure, and the Federal Government in order to enhance the ability of recipients of such information to ensure the protection and defense of public, private, and critical infrastructure information networks; and

(4) coordinate with the private sector, State, tribal, and local governments, the governments of foreign countries, international organizations, and academic institutions in developing and encouraging the use of voluntary standards for enhancing the security of information networks.

SEC. 204. BOARD OF DIRECTORS.

(a) IN GENERAL.—The Cyber Defense Alliance shall have a Board of Directors which shall be responsible for—

(1) the executive and administrative operation of the Alliance, including matters relating to funding and promotion of the Alliance; and

(2) ensuring and facilitating compliance by members of the Alliance with the requirements of this title.

(b) COMPOSITION.—The Board shall be composed of the following members:

(1) One representative of the Department of Energy.

(2) Four representatives of Federal agencies, other than the Department of Energy, that have significant responsibility for the protection or defense of government information networks.

(3) Two representatives from the private sector.

(4) Two representatives of State, tribal, and local government departments, agencies, or entities.

(5) Two representatives from the financial sector.

(6) Two representatives from electronic communication service providers.

(7) Two representatives from the transportation industry.

(8) Two representatives from the chemical industry.

(9) Two representatives from a public or private electric utility company or other generators of power.

(10) One representative from an academic institution with established expertise in cyber-related matters.

(11) One additional representative with considerable expertise in cyber-related matters.

(c) INITIAL APPOINTMENT.—Not later than 30 days after the date of the enactment of this Act, the Director

of the National Cyber Center, the Secretary of Energy, the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation shall jointly appoint the members of the Board described under subsection (b).

(d) TERMS.—

(1) REPRESENTATIVES OF CERTAIN FEDERAL AGENCIES.—Each member of the Board described in subsection (b)(1) shall serve for a term that is—

(A) not longer than three years from the date of the member's appointment; and

(B) determined jointly by the Director of the National Cyber Center, the Secretary of Energy, the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation.

(2) OTHER REPRESENTATIVES.—The original members of the Board described in paragraphs (3) through (11) of subsection (b) shall serve an initial term of one year from the date of appointment under subsection (c), at which time the members of the Cyber Defense Alliance shall conduct elections in

accordance with the procedures established under subsection (e).

(e) RULES AND PROCEDURES.—Not later than 90 days after the date of the enactment of this Act, the Board shall establish rules and procedures for the election and service of members of the Board described in paragraphs (3) through (11) of subsection (b).

(f) LEADERSHIP.—The Board shall elect from among its members a chair and co-chair of the Board, who shall serve under such terms and conditions as the Board may establish.

(g) SUB-BOARDS.—The Board shall have the authority to constitute such sub-Boards, or other advisory groups or panels, from among the members of the Board as may be necessary to assist the Board in carrying out its functions under this section.

SEC. 205. CYBER DEFENSE ALLIANCE MEMBERSHIP.

(a) REQUIREMENT FOR PROCEDURES.—Not later than 90 days after the date of the enactment of this Act, the Board shall establish procedures for the voluntary membership by State, tribal, and local government departments, agencies, and entities, private sector businesses and organizations, and academic institutions in the Cyber Defense Alliance.

(b) PARTICIPATION BY FEDERAL AGENCIES.—The Director of the National Cyber Center, in coordination with the Secretary of Energy, the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, the Director of the Federal Bureau of Investigation, and the heads of other appropriate Federal agencies, may provide for the participation and cooperation of such Federal agencies in the Cyber Defense Alliance.

SEC. 206. FUNDING.

(a) INITIAL EXPENSES.—Administrative and logistical expenses associated with the initial establishment of the Cyber Defense Alliance shall be paid by the Secretary of Energy and shall be included within the National Cyber Security Program budget request for the Department of Energy.

(b) OTHER EXPENSES.—

(1) IN GENERAL.—Except as provided in paragraph (2), annual administrative and operational expenses for the Cyber Defense Alliance shall be paid by the members of such Alliance, as determined by the Board.

(2) MAXIMUM FEDERAL CONTRIBUTION.—Not more than 15 percent of the annual expenses referred to in paragraph (1) may be paid by the Fed-

eral Government. Such amount shall be provided under the direction of the Secretary of Energy and shall be included within the National Cyber Security Program budget request for the Department of Energy.

SEC. 207. CLASSIFIED INFORMATION.

Consistent with the protection of sensitive intelligence sources and methods, the Director of National Intelligence shall facilitate—

(1) the sharing of classified information in the possession of a Federal agency related to threats to information networks with appropriately cleared members of the Alliance, including representatives of the private sector and of public and private sector entities operating critical infrastructure; and

(2) the declassification and sharing of information in the possession of a Federal agency related to threats to information networks with members of the Alliance.

SEC. 208. VOLUNTARY INFORMATION SHARING.

(a) USES OF SHARED INFORMATION.—

(1) IN GENERAL.—Notwithstanding any other provision of law and subject to paragraph (2), information shared with or provided to the Cyber Defense Alliance or to a Federal agency through such

Alliance by any member of the Cyber Defense Alliance that is not a Federal agency in furtherance of the mission and activities of the Alliance as described in section 203—

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to the rules of any Federal agency or any judicial doctrine regarding ex parte communications with a decision-making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal agency, any other Federal, State, tribal, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted to the Cyber Defense Alliance in good faith and for the purpose of facilitating the missions of such Alliance;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or

employee of the United States for purposes other than the purposes of this title, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) the disclosure of the information to the appropriate congressional committee;

(E) shall not, if subsequently provided to a State, tribal, or local government or government agency—

(i) be made available pursuant to any State, tribal, or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by such State, tribal, or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting information systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) APPLICATION.—Paragraph (1) shall only apply to information shared with or provided to the Cyber Defense Alliance or to a Federal agency through such Alliance by a member of the Cyber Defense Alliance that is not a Federal agency if such information is accompanied by an express statement requesting that such paragraph apply.

(b) LIMITATION.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to any communication of information to a Federal agency made pursuant to this title.

(c) PROCEDURES.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the heads of appropriate Federal agencies, establish uniform procedures for the receipt, care, and storage by such agencies of information that is voluntarily submitted to the Federal Government through the Cyber Defense Alliance.

(2) ELEMENTS.—The procedures established under paragraph (1) shall include procedures for—

(A) the acknowledgment of receipt by a Federal agency of cyber threat information that

is voluntarily submitted to the Federal Government;

(B) the maintenance of the identification of such information;

(C) the care and storage of such information;

(D) limiting subsequent dissemination of such information to ensure that such information is not used for an unauthorized purpose;

(E) the protection of the constitutional and statutory rights of any individuals who are subjects of such information; and

(F) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State, tribal, and local governments, and the issuance of notices and warnings related to the protection of information networks, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(d) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a Federal agency, a State, tribal, or local government or government agency, or any third party—

(1) to obtain cyber threat information in a manner other than through the Cyber Defense Alliance, including obtaining any information lawfully and properly disclosed generally or broadly to the public; and

(2) to use such information in any manner permitted by law.

SEC. 209. PENALTIES.

(a) IN GENERAL.—It shall be unlawful for any officer or employee of the United States or of any Federal agency to knowingly publish, divulge, disclose, or make known in any manner or to any extent not authorized by law, any cyber threat information protected from disclosure by this title coming to such officer or employee in the course of the employee's employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such officer, employee, or agency.

(b) PENALTY.—Any person who violates subsection (a) shall be fined under title 18, United States Code, im-

prisoned for not more than 1 year, or both, and shall be removed from office or employment.

SEC. 210. AUTHORITY TO ISSUE WARNINGS.

The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to information networks as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted information that forms the basis for the warning; and

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

SEC. 211. EXEMPTION FROM ANTITRUST PROHIBITIONS.

The exchange of information by and between private sector members of the Cyber Defense Alliance, in furtherance of the mission and activities of the Cyber Defense Alliance, shall not be considered a violation of any provision of the antitrust laws (as defined in the first section of the Clayton Act (15 U.S.C. 12)).

SEC. 212. DURATION.

The Cyber Defense Alliance shall cease to exist on December 31, 2020.

○