

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “National Cyber Infra-
5 structure Protection Act of 2010”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) APPROPRIATE CONGRESSIONAL COMMIT-
9 TEES.—The term “appropriate congressional com-
10 mittees” means—

1 (A) the Committee on Armed Services, the
2 Committee on Commerce, Science, and Trans-
3 portation, the Committee on Energy and Nat-
4 ural Resources, the Committee on Homeland
5 Security and Governmental Affairs, and the Se-
6 lect Committee on Intelligence of the Senate;
7 and

8 (B) the Committee on Armed Services, the
9 Committee on Energy and Commerce, the Com-
10 mittee on Homeland Security, and the Perma-
11 nent Select Committee on Intelligence of the
12 House of Representatives.

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

17 (3) CYBER SECURITY ACTIVITIES.—The term
18 “cyber security activities” means a class or collection
19 of similar cyber security operations of a Federal
20 agency that involves personally identifiable data that
21 is—

22 (A) screened by a cyber security system
23 outside of the Federal agency that was the in-
24 tended recipient of the personally identifiable
25 data;

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

3 (C) transferred, for the purpose of cyber
4 security, to an element of the intelligence com-
5 munity.

6 (4) FEDERAL AGENCY.—The term “Federal
7 agency” has the meaning given the term “Executive
8 agency” in section 105 of title 5, United States
9 Code.

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

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

18 (7) NATIONAL CYBER SECURITY PROGRAM.—
19 The term “National Cyber Security Program”
20 means the programs, projects, and activities of the
21 Federal Government to protect and defend Federal
22 Government information networks and to facilitate
23 the protection and defense of United States informa-
24 tion networks.

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

5 (9) STATE.—The term “State” means—

6 (A) a State;

7 (B) the District of Columbia;

8 (C) the Commonwealth of Puerto Rico;

9 and

10 (D) any other territory or possession of the

11 United States.

12 **TITLE I—NATIONAL CYBER** 13 **CENTER**

14 **SEC. 101. DIRECTOR DEFINED.**

15 In this title, except as otherwise specifically provided,
 16 the term “Director” means the Director of the National
 17 Cyber Center appointed under section 103.

18 **SEC. 102. ESTABLISHMENT OF THE NATIONAL CYBER CEN-** 19 **TER.**

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

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

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

3 **SEC. 103. DIRECTOR OF THE NATIONAL CYBER CENTER.**

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

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

12 (c) REPORTING AND PLACEMENT.—

13 (1) REPORTING.—The Director shall report di-
14 rectly to the President.

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

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

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

24 (2) act as the principal adviser to the Presi-
25 dent, the National Security Council, and to the

1 heads of Federal agencies on matters relating to the
2 protection and defense of Federal Government infor-
3 mation networks;

4 (3) coordinate, and ensure the adequacy of, the
5 National Cyber Security Program budgets for Fed-
6 eral agencies;

7 (4) maintain and disperse funds from the Na-
8 tional Cyber Defense Contingency Fund in accord-
9 ance with section 108;

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

14 (6) ensure appropriate coordination within the
15 Federal Government for the conduct of any oper-
16 ations, strategies, and intelligence collection and
17 analysis relating to the protection and defense of
18 Federal Government information networks;

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

1 (8) provide assistance to, and cooperate with,
2 the Cyber Defense Alliance established under section
3 202, including the development of partnerships with
4 public and private sector entities, and academic in-
5 stitutions that encourage cooperation, research, de-
6 velopment, and cyber security education and train-
7 ing;

8 (9) develop plans and policies for the security of
9 Federal Government information networks to be im-
10 plemented by the appropriate Federal agency;

11 (10) participate in the process to develop reli-
12 ability standards pursuant to section 215 of the
13 Federal Power Act (16 U.S.C. 824o);

14 (11) develop plans and policies for the sharing
15 of cyber threat-related information among appro-
16 priate Federal agencies, and to the extent consistent
17 with the protection of national security sources and
18 methods, with State, tribal, and local government
19 departments, agencies, and entities, and public and
20 private sector entities that operate critical infra-
21 structure;

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

1 (13) perform such other functions as may be di-
2 rected by the President.

3 **SEC. 104. MISSIONS OF THE NATIONAL CYBER CENTER.**

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

6 (1) serve as the primary organization for co-
7 ordinating Federal Government defensive operations,
8 intelligence collection and analysis, and activities to
9 protect and defend Federal Government information
10 networks;

11 (2) develop policies and procedures for imple-
12 mentation across the Federal Government on mat-
13 ters relating to the protection and defense of Fed-
14 eral Government information networks;

15 (3) provide a process for resolving conflicts
16 among Federal agencies relating to the implementa-
17 tion of cyber security activities or the conduct of op-
18 erations, strategies, and intelligence collection and
19 analysis relating to the protection and defense of
20 Federal Government information networks;

21 (4) assign roles and responsibilities to Federal
22 agencies, as appropriate, for the protection and de-
23 fense of Federal Government information networks
24 that are consistent with applicable law; and

1 (5) ensure that, as appropriate, Federal agen-
2 cies have access to, and receive, information, includ-
3 ing appropriate private sector information, regarding
4 cyber threats to Federal Government information
5 networks.

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

9 (1) except as otherwise provided by law;

10 (2) unless otherwise directed by the President;

11 or

12 (3) unless the Attorney General and the Direc-
13 tor agree on guidelines to limit such access.

14 **SEC. 105. COMPOSITION OF NATIONAL CYBER CENTER.**

15 (a) INTEGRATION OF RESOURCES.—Not later than
16 90 days after the date of the confirmation of the initial
17 Director, the Secretary of Defense, the Secretary of
18 Homeland Security, the Director of National Intelligence,
19 and the Director of the Federal Bureau of Investigation
20 shall, in consultation with the Director, collocate and inte-
21 grate within the National Cyber Center such elements, of-
22 fices, task forces, and other components of the Depart-
23 ment of Defense, the Department of Homeland Security,
24 the intelligence community, and the Federal Bureau of In-

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

3 (b) PARTICIPATION OF FEDERAL AGENCIES.—Any
4 Federal agency not referred to in subsection (a) may par-
5 ticipate in the National Cyber Center if the head of such
6 Federal agency and the Director agree on the level and
7 type of such participation.

8 (c) RECOMMENDATIONS FOR CONSOLIDATION.—In
9 order to reduce duplication of Federal Government efforts,
10 the Director may recommend that the President transfer
11 to, and consolidate within, the National Cyber Center ac-
12 tivities that relate to the protection and defense of Federal
13 Government information networks.

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

22 **SEC. 106. NATIONAL CYBER CENTER OFFICIALS.**

23 (a) DEPUTY DIRECTOR.—

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

4 (2) APPOINTMENT CRITERIA.—An individual
5 appointed Deputy Director of the National Cyber
6 Center shall have extensive cyber security and man-
7 agement expertise.

8 (3) DUTIES.—The Deputy Director shall—

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

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

15 (b) GENERAL COUNSEL.—

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

19 (2) DUTIES.—The General Counsel is the chief
20 legal officer of the National Cyber Center and shall
21 perform such functions as the Director may pre-
22 scribe.

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

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

7 **SEC. 107. NATIONAL CYBER SECURITY PROGRAM BUDGET.**

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

19 (b) REVIEW AND CERTIFICATION OF BUDGET RE-
 20 QUESTS AND BUDGET SUBMISSIONS.—

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

24 (2) REVIEW OF BUDGET REQUESTS.—

1 (A) INADEQUATE REQUESTS.—If the Di-
2 rector concludes that a budget request sub-
3 mitted under subsection (a) for a Federal agen-
4 cy is inadequate to accomplish the protection
5 and defense of Federal Government information
6 networks, or to facilitate the protection and de-
7 fense of United States information networks,
8 with respect to such Federal agency for the
9 year for which the request is submitted, the Di-
10 rector shall submit to the head of such Federal
11 agency a written description of funding levels
12 and specific initiatives that would, in the deter-
13 mination of the Director, make the request ade-
14 quate to accomplish the protection and defense
15 of such information networks.

16 (B) ADEQUATE REQUESTS.—If the Direc-
17 tor concludes that a budget request submitted
18 under subsection (a) for a Federal agency is
19 adequate to accomplish the protection and de-
20 fense of Federal Government information net-
21 works, or to facilitate the protection and de-
22 fense of United States information networks,
23 with respect to such Federal agency for the
24 year for which the request is submitted, the Di-
25 rector shall submit to the head of such Federal

1 agency a written statement confirming the ade-
2 quacy of the request.

3 (C) RECORD.—The Director shall maintain
4 a record of each description submitted under
5 subparagraph (A) and each statement sub-
6 mitted under subparagraph (B).

7 (3) AGENCY RESPONSE.—

8 (A) IN GENERAL.—The head of a Federal
9 agency that receives a description under para-
10 graph (2)(A) shall include the funding levels
11 and initiatives described by the Director in the
12 National Cyber Security Program budget sub-
13 mission for such Federal agency to the Office of
14 Management and Budget.

15 (B) IMPACT STATEMENT.—If the head of a
16 Federal agency alters the National Cyber Secu-
17 rity Program budget submission of such agency
18 based on a description received under para-
19 graph (2)(A), such head shall include as an ap-
20 pendix to the budget submitted to the Office of
21 Management and Budget for such agency an
22 impact statement that summarizes—

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

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

6 (4) CONGRESSIONAL NOTIFICATION.—The head
7 of a Federal agency shall submit to Congress a copy
8 of any impact statement prepared under paragraph
9 (3)(B) at the time the National Cyber Security Pro-
10 gram budget for such agency is submitted to Con-
11 gress under section 1105(a) of title 31, United
12 States Code.

13 (5) CERTIFICATION OF NATIONAL CYBER SECUR-
14 ITY PROGRAM BUDGET SUBMISSIONS.—

15 (A) IN GENERAL.—At the time the head of
16 a Federal agency submits a National Cyber Se-
17 curity Program budget request for such agency
18 for a fiscal year to the Office of Management
19 and Budget, such head shall submit a copy of
20 the National Cyber Security Program budget
21 request to the Director.

22 (B) DECERTIFICATION.—

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

1 gram budget request submitted under sub-
2 paragraph (A).

3 (ii) BUDGET DECERTIFICATION.—If,
4 based on the review under clause (i), the
5 Director concludes that such budget re-
6 quest does not include the funding levels
7 and specific initiatives that would, in the
8 determination of the Director, make the
9 request adequate to accomplish the protec-
10 tion and defense of Federal Government
11 information networks, or to facilitate the
12 protection and defense of United States in-
13 formation networks, the Director may
14 issue a written decertification of such Fed-
15 eral agency’s budget.

16 (iii) SUBMISSION TO CONGRESS.—In
17 the case of a decertification of a budget re-
18 quest issued under clause (ii), the Director
19 shall submit to Congress a copy of—

20 (I) such National Cyber Security
21 Program budget request;

22 (II) such decertification; and

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

1 (c) CONSOLIDATED NATIONAL CYBER SECURITY
2 PROGRAM BUDGET PROPOSAL.—For each fiscal year, fol-
3 lowing the transmission of proposed National Cyber Secu-
4 rity Program budget requests for Federal agencies to the
5 Director under subsection (a), the Director shall, in con-
6 sultation with the head of such Federal agencies—

7 (1) develop a consolidated National Cyber Secu-
8 rity Program budget proposal;

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

11 (3) after making the submission required by
12 paragraph (2), submit the consolidated budget pro-
13 posal to Congress.

14 **SEC. 108. NATIONAL CYBER DEFENSE CONTINGENCY FUND.**

15 (a) ESTABLISHMENT OF FUND.—There is estab-
16 lished within the National Cyber Security Program Budg-
17 et a fund to be known as the “National Cyber Defense
18 Contingency Fund,” which shall consist of amounts appro-
19 priated to the Fund for the purpose of providing financial
20 assistance and technical and operational support in the
21 event of a significant cyber incident.

22 (b) ADMINISTRATION.—The Director shall be respon-
23 sible for the administration and management of the
24 amounts in the National Cyber Defense Contingency
25 Fund.

1 (c) USE.—In response to a significant cyber incident
 2 involving Federal Government or United States informa-
 3 tion networks, the Director may distribute amounts from
 4 the National Cyber Defense Contingency Fund to appro-
 5 priate Federal agencies.

6 (d) NOTIFICATION.—Prior to distributing amounts
 7 under this section, the Director shall notify the appro-
 8 priate congressional committees.

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

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

14 (2) affects one or more Federal agencies or
 15 public or private sector entities operating critical in-
 16 frastructure;

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

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

21 **SEC. 109. PROGRAM BUDGET SUBMISSION.**

22 (a) SUBMISSION.—Section 1105(a) of title 31, United
 23 States Code, is amended by adding at the end the fol-
 24 lowing:

1 “(38) a separate statement of the combined and
2 individual amounts of appropriations requested for
3 the National Cyber Security Program, including a
4 separate statement of the amounts of appropriations
5 requested by the Secretary of Defense for the oper-
6 ation and activities of the National Cyber Center
7 and a separate statement of the amounts of appro-
8 priations requested by the Secretary of Energy for
9 the operation and activities of the Cyber Defense Al-
10 liance.”.

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

14 (1) by redesignating the paragraph (33) added
15 by section 889 of the Homeland Security Act of
16 2002 (Public Law 107–296; 116 Stat. 2250) as
17 paragraph (35);

18 (2) by redesignating the paragraph (35) added
19 by section 203 of the Emergency Economic Sta-
20 bilization Act of 2008 (division A of Public Law
21 110–343; 122 Stat. 3765) as paragraph (36); and

22 (3) by redesignating the paragraph (36) added
23 by section 2 of the Veterans Health Care Budget
24 Reform and Transparency Act of 2009 (Public Law
25 111–81; 123 Stat. 2137) as paragraph (37).

1 **SEC. 110. CONSTRUCTION.**

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

7 **SEC. 111. CONGRESSIONAL OVERSIGHT.**

8 The Director shall keep the appropriate congressional
 9 committees fully and currently informed of the significant
 10 activities of the National Cyber Center relating to ensur-
 11 ing the security of Federal Government information net-
 12 works.

13 **TITLE II—CYBER DEFENSE**
 14 **ALLIANCE**

15 **SEC. 201. DEFINITIONS.**

16 In this title:

17 (1) BOARD.—The term “Board” means the
 18 Board of Directors of the Cyber Defense Alliance es-
 19 tablished pursuant to section 204(a).

20 (2) NATIONAL LABORATORY.—The term “Na-
 21 tional Laboratory” has the meaning given that term
 22 in section 2 of the Energy Policy Act of 2005 (42
 23 U.S.C. 15801).

24 **SEC. 202. CYBER DEFENSE ALLIANCE.**

25 (a) CHARTER.—There is within a National Labora-
 26 tory a public and private partnership for sharing cyber

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

4 (b) ESTABLISHMENT.—The Secretary of Energy, in
5 coordination with the Director of the National Cyber Cen-
6 ter, the Director of National Intelligence, the Secretary
7 of Defense, the Secretary of Homeland Security, and the
8 Director of the Federal Bureau of Investigation, shall de-
9 termine the appropriate location for, and establish, the
10 Cyber Defense Alliance.

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

14 (1) Whether the National Laboratory has re-
15 ceived recognition from members of the intelligence
16 community, the Secretary of Homeland Security, or
17 the Secretary of Defense for its cyber capabilities.

18 (2) Whether the National Laboratory has dem-
19 onstrated the ability to address cyber-related issues
20 involving varying levels of classified information.

21 (3) Whether the National Laboratory has dem-
22 onstrated the capability to develop cooperative rela-
23 tionships with the private sector on cyber-related
24 issues.

1 (d) PARTNERSHIP.—If the Secretary of Energy, the
2 Director of the National Cyber Center, the Director of Na-
3 tional Intelligence, the Secretary of Defense, the Secretary
4 of Homeland Security, and the Director of the Federal
5 Bureau of Investigation determine that the missions and
6 activities of the Cyber Defense Alliance may only be ac-
7 complished through a partnership of two or more National
8 Laboratories acting jointly to support the Alliance, then
9 the Alliance may be established and located within such
10 National Laboratories.

11 **SEC. 203. MISSION AND ACTIVITIES.**

12 The Cyber Defense Alliance shall—

13 (1) facilitate the exchange of ideas and tech-
14 nical assistance and support related to the security
15 of public, private, and critical infrastructure infor-
16 mation networks;

17 (2) promote research and development, includ-
18 ing the advancement of private funding for research
19 and development, related to ensuring the security of
20 public, private, and critical infrastructure informa-
21 tion networks;

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

1 tor entities operating critical infrastructure, and the
 2 Federal Government in order to enhance the ability
 3 of recipients of such information to ensure the pro-
 4 tection and defense of public, private, and critical in-
 5 frastructure information networks; and

6 (4) coordinate with the private sector, State,
 7 tribal, and local governments, the governments of
 8 foreign countries, international organizations, and
 9 academic institutions in developing and encouraging
 10 the use of voluntary standards for enhancing the se-
 11 curity of information networks.

12 **SEC. 204. BOARD OF DIRECTORS.**

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

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

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

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

23 (1) One representative of the Department of
 24 Energy.

1 (2) Four representatives of Federal agencies,
2 other than the Department of Energy, that have sig-
3 nificant responsibility for the protection or defense
4 of government information networks.

5 (3) Two representatives from the private sector.

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

8 (5) Two representatives from the financial sec-
9 tor.

10 (6) Two representatives from electronic commu-
11 nication service providers.

12 (7) Two representatives from the transportation
13 industry.

14 (8) Two representatives from the chemical in-
15 dustry.

16 (9) Two representatives from a public or pri-
17 vate electric utility company or other generators of
18 power.

19 (10) One representative from an academic insti-
20 tution with established expertise in cyber-related
21 matters.

22 (11) One additional representative with consid-
23 erable expertise in cyber-related matters.

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

1 of the National Cyber Center, the Secretary of Energy,
2 the Director of National Intelligence, the Secretary of De-
3 fense, the Secretary of Homeland Security, and the Direc-
4 tor of the Federal Bureau of Investigation shall jointly ap-
5 point the members of the Board described under sub-
6 section (b).

7 (d) TERMS.—

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

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

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

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

1 accordance with the procedures established under
2 subsection (e).

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

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

12 (g) SUB-BOARDS.—The Board shall have the author-
13 ity to constitute such sub-Boards, or other advisory groups
14 or panels, from among the members of the Board as may
15 be necessary to assist the Board in carrying out its func-
16 tions under this section.

17 **SEC. 205. CYBER DEFENSE ALLIANCE MEMBERSHIP.**

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

1 (b) PARTICIPATION BY FEDERAL AGENCIES.—The
2 Director of the National Cyber Center, in coordination
3 with the Secretary of Energy, the Director of National In-
4 telligence, the Secretary of Defense, the Secretary of
5 Homeland Security, the Director of the Federal Bureau
6 of Investigation, and the heads of other appropriate Fed-
7 eral agencies, may provide for the participation and co-
8 operation of such Federal agencies in the Cyber Defense
9 Alliance.

10 **SEC. 206. FUNDING.**

11 (a) INITIAL EXPENSES.—Administrative and
12 logistical expenses associated with the initial establishment
13 of the Cyber Defense Alliance shall be paid by the Sec-
14 retary of Energy and shall be included within the National
15 Cyber Security Program budget request for the Depart-
16 ment of Energy.

17 (b) OTHER EXPENSES.—

18 (1) IN GENERAL.—Except as provided in para-
19 graph (2), annual administrative and operational ex-
20 penses for the Cyber Defense Alliance shall be paid
21 by the members of such Alliance, as determined by
22 the Board.

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

1 eral Government. Such amount shall be provided
2 under the direction of the Secretary of Energy and
3 shall be included within the National Cyber Security
4 Program budget request for the Department of En-
5 ergy.

6 **SEC. 207. CLASSIFIED INFORMATION.**

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

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

16 (2) the declassification and sharing of informa-
17 tion in the possession of a Federal agency related to
18 threats to information networks with members of the
19 Alliance.

20 **SEC. 208. VOLUNTARY INFORMATION SHARING.**

21 (a) USES OF SHARED INFORMATION.—

22 (1) IN GENERAL.—Notwithstanding any other
23 provision of law and subject to paragraph (2), infor-
24 mation shared with or provided to the Cyber De-
25 fense Alliance or to a Federal agency through such

1 Alliance by any member of the Cyber Defense Alli-
2 ance that is not a Federal agency in furtherance of
3 the mission and activities of the Alliance as de-
4 scribed in section 203—

5 (A) shall be exempt from disclosure under
6 section 552 of title 5, United States Code (com-
7 monly referred to as the Freedom of Informa-
8 tion Act);

9 (B) shall not be subject to the rules of any
10 Federal agency or any judicial doctrine regard-
11 ing ex parte communications with a decision-
12 making official;

13 (C) shall not, without the written consent
14 of the person or entity submitting such infor-
15 mation, be used directly by any Federal agency,
16 any other Federal, State, tribal, or local author-
17 ity, or any third party, in any civil action aris-
18 ing under Federal or State law if such informa-
19 tion is submitted to the Cyber Defense Alliance
20 in good faith and for the purpose of facilitating
21 the missions of such Alliance;

22 (D) shall not, without the written consent
23 of the person or entity submitting such infor-
24 mation, be used or disclosed by any officer or

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

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

5 (ii) the disclosure of the information
6 to the appropriate congressional com-
7 mittee;

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

11 (i) be made available pursuant to any
12 State, tribal, or local law requiring disclo-
13 sure of information or records;

14 (ii) otherwise be disclosed or distrib-
15 uted to any party by such State, tribal, or
16 local government or government agency
17 without the written consent of the person
18 or entity submitting such information; or

19 (iii) be used other than for the pur-
20 pose of protecting information systems, or
21 in furtherance of an investigation or the
22 prosecution of a criminal act; and

23 (F) does not constitute a waiver of any ap-
24 plicable privilege or protection provided under
25 law, such as trade secret protection.

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

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

12 (c) PROCEDURES.—

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

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

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

1 is voluntarily submitted to the Federal Govern-
2 ment;

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

5 (C) the care and storage of such informa-
6 tion;

7 (D) limiting subsequent dissemination of
8 such information to ensure that such informa-
9 tion is not used for an unauthorized purpose;

10 (E) the protection of the constitutional and
11 statutory rights of any individuals who are sub-
12 jects of such information; and

13 (F) the protection and maintenance of the
14 confidentiality of such information so as to per-
15 mit the sharing of such information within the
16 Federal Government and with State, tribal, and
17 local governments, and the issuance of notices
18 and warnings related to the protection of infor-
19 mation networks, in such manner as to protect
20 from public disclosure the identity of the sub-
21 mitting person or entity, or information that is
22 proprietary, business sensitive, relates specifi-
23 cally to the submitting person or entity, and is
24 otherwise not appropriately in the public do-
25 main.

1 (d) INDEPENDENTLY OBTAINED INFORMATION.—

2 Nothing in this section shall be construed to limit or other-
3 wise affect the ability of a Federal agency, a State, tribal,
4 or local government or government agency, or any third
5 party—

6 (1) to obtain cyber threat information in a
7 manner other than through the Cyber Defense Alli-
8 ance, including obtaining any information lawfully
9 and properly disclosed generally or broadly to the
10 public; and

11 (2) to use such information in any manner per-
12 mitted by law.

13 **SEC. 209. PENALTIES.**

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

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

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

3 **SEC. 210. AUTHORITY TO ISSUE WARNINGS.**

4 The Federal Government may provide advisories,
5 alerts, and warnings to relevant companies, targeted sec-
6 tors, other government entities, or the general public re-
7 garding potential threats to information networks as ap-
8 propriate. In issuing a warning, the Federal Government
9 shall take appropriate actions to protect from disclosure—

10 (1) the source of any voluntarily submitted in-
11 formation that forms the basis for the warning; and

12 (2) information that is proprietary, business
13 sensitive, relates specifically to the submitting per-
14 son or entity, or is otherwise not appropriately in
15 the public domain.

16 **SEC. 211. EXEMPTION FROM ANTITRUST PROHIBITIONS.**

17 The exchange of information by and between private
18 sector members of the Cyber Defense Alliance, in further-
19 ance of the mission and activities of the Cyber Defense
20 Alliance, shall not be considered a violation of any provi-
21 sion of the antitrust laws (as defined in the first section
22 of the Clayton Act (15 U.S.C. 12)).

1 **SEC. 212. DURATION.**

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

○