

[DISCUSSION DRAFT]

112TH CONGRESS
1ST SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. DANIEL E. LUNGREN of California introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, 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
5 “_____ Act of 2011”.

1 **SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBERSE-**
2 **CURITY ACTIVITIES.**

3 (a) IN GENERAL.—Subtitle C of title II of the Home-
4 land Security Act of 2002 is amended by adding at the
5 end the following new sections:

6 **“SEC. 226. NATIONAL CYBERSECURITY AUTHORITY.**

7 “(a) IN GENERAL.—To protect Federal systems and
8 critical infrastructure information systems and to prepare
9 the Nation to respond to, recover from, and mitigate
10 against acts of terrorism and other incidents involving
11 such systems and infrastructure, the Secretary shall—

12 “(1) develop and conduct risk assessments for
13 Federal systems and, upon request, critical infra-
14 structure information systems in consultation with
15 the heads of other agencies or governmental and pri-
16 vate entities that own and operate such systems,
17 that may include threat, vulnerability, and impact
18 assessments and penetration testing, or other com-
19 prehensive assessments techniques;

20 “(2) foster the development, in conjunction with
21 other governmental entities and the private sector,
22 of essential information security technologies and ca-
23 pabilities for protecting Federal systems and critical
24 infrastructure information systems, including com-
25 prehensive protective capabilities and other techno-
26 logical solutions;

1 “(3) acquire, integrate, and facilitate the adop-
2 tion of new cybersecurity technologies and practices
3 to keep pace with emerging terrorist and other cy-
4 bersecurity threats and developments, including
5 through research and development, technical service
6 agreements, and making such technologies available
7 to governmental and private entities that own or op-
8 erate critical infrastructure information systems, as
9 necessary to accomplish the purpose of this section;

10 “(4) maintain the capability to serve as a focal
11 point with the Federal Government for cybersecu-
12 rity, responsible for—

13 “(A) the protection of Federal systems and
14 critical infrastructure information systems;

15 “(B) the coordination of cyber incident re-
16 sponse;

17 “(C) facilitating information sharing, inter-
18 actions, and collaborations among and between
19 Federal agencies, State and local governments,
20 the private sector, academia, and international
21 partners;

22 “(D) working with appropriate Federal
23 agencies, State and local governments, the pri-
24 vate sector, academia, and international part-
25 ners to prevent and respond to terrorist and

1 other cybersecurity threats and incidents involv-
2 ing Federal systems and critical infrastructure
3 information systems pursuant to the national
4 cyber incident response plan and supporting
5 plans developed in accordance with paragraph
6 (8);

7 “(E) the dissemination of timely and ac-
8 tionable terrorist and other cybersecurity
9 threat, vulnerability, mitigation, and warning
10 information, including alerts, advisories, indica-
11 tors, signatures, and mitigation and response
12 measures, to improve the security and protec-
13 tion of Federal systems and critical infrastruc-
14 ture information systems;

15 “(F) the integration of information from
16 Federal Government and non-federal network
17 operation centers and security operations cen-
18 ters;

19 “(G) the compilation and analysis of infor-
20 mation about risks and incidents regarding ter-
21 rorism or other causes that threaten Federal
22 systems and critical infrastructure information
23 systems; and

24 “(H) the provision of incident detection,
25 analysis, mitigation, and response information

1 and remote or on-site technical assistance to
2 heads of Federal agencies and, upon request,
3 governmental and private entities that own or
4 operate critical infrastructure;

5 “(5) assist in national efforts to mitigate com-
6 munications and information technology supply
7 chain vulnerabilities to enhance the security and the
8 resiliency of Federal systems and critical infrastruc-
9 ture information systems;

10 “(6) develop and lead a nationwide awareness
11 and outreach effort to educate the public about—

12 “(A) the importance of cybersecurity;

13 “(B) ways to promote cybersecurity best
14 practices at home and in the workplace; and

15 “(C) training opportunities to support the
16 development of an effective national cybersecu-
17 rity workforce and educational paths to cyberse-
18 curity professions;

19 “(7) establish, in coordination with the Director
20 of the National Institute of Standards and Tech-
21 nology and the heads of other appropriate agencies,
22 benchmarks and guidelines for making critical infra-
23 structure information systems more secure at a fun-
24 damental level, including through automation, inter-
25 operability, and privacy-enhancing authentication;

1 “(8) develop a national cybersecurity incident
2 response plan and supporting cyber incident re-
3 sponse and restoration plans, in consultation with
4 the heads of other relevant Federal agencies, owners
5 and operators of critical infrastructure, sector co-
6 ordinating councils, State and local governments,
7 and relevant non-governmental organizations and
8 based on applicable law that describe the specific
9 roles and responsibilities of governmental and pri-
10 vate entities during cyber incidents;

11 “(9) develop and conduct exercises, simulations,
12 and other activities designed to support the national
13 response to terrorism and other cybersecurity
14 threats and incidents and evaluate the national
15 cyber incident response plan and supporting plans
16 developed in accordance with paragraph (8); and

17 “(10) take such other lawful action as may be
18 necessary and appropriate to accomplish the require-
19 ments of this section.

20 “(b) COORDINATION.—

21 “(1) COORDINATION WITH OTHER ENTITIES.—

22 In carrying out the cybersecurity activities under
23 this section, the Secretary shall coordinate, as ap-
24 propriate, with—

1 “(A) the head of any relevant agency or
2 entity;

3 “(B) representatives of State and local
4 governments;

5 “(C) the private sector, including owners
6 and operators of critical infrastructure;

7 “(D) suppliers of technology for critical in-
8 frastructure;

9 “(E) academia; and

10 “(F) international organizations and for-
11 eign partners.

12 “(2) COORDINATION OF AGENCY ACTIVITIES.—

13 The Secretary shall coordinate the activities under-
14 taken by agencies to protect Federal systems and
15 critical infrastructure information systems and pre-
16 pare the Nation to respond to, recover from, and
17 mitigate against risk of acts of terrorism and other
18 incidents involving such systems and infrastructure.

19 “(3) LEAD CYBERSECURITY OFFICIAL.—The

20 Secretary shall designate a lead cybersecurity official
21 to provide leadership to the cybersecurity activities
22 of the Department and to ensure that the Depart-
23 ment’s cybersecurity activities under this subtitle are
24 coordinated with all other infrastructure protection
25 and cyber-related programs and activities of the De-

1 partment, including those of any intelligence or law
2 enforcement components or entities within the De-
3 partment.

4 “(4) REPORTS TO CONGRESS.—The lead cyber-
5 security official shall make regular reports to the ap-
6 propriate committees of Congress on the coordina-
7 tion of cyber-related programs across the Depart-
8 ment.

9 “(c) STRATEGY.—In carrying out the cybersecurity
10 functions of the Department, the Secretary shall develop
11 and maintain a strategy that—

12 “(1) articulates the actions necessary to assure
13 the readiness, reliability, continuity, integrity, and
14 resilience of Federal systems and critical infrastruc-
15 ture information systems;

16 “(2) enhances economic prosperity and facili-
17 tates market leadership for the United States infor-
18 mation and communications industry; and

19 “(3) protects privacy rights and preserves civil
20 liberties of United States persons.

21 “(d) NO RIGHT OR BENEFIT.—The provision of as-
22 sistance or information to governmental or private entities
23 that own or operate critical infrastructure information sys-
24 tems under this section shall be at the discretion of the
25 Secretary and subject to the availability of resources. The

1 provision of certain assistance or information to one gov-
2 ernmental or private entity pursuant to this section shall
3 not create a right or benefit, substantive or procedural,
4 to similar assistance or information for any other govern-
5 mental or private entity.

6 “(e) SAVINGS CLAUSE.—Nothing in this subtitle shall
7 be interpreted to alter or amend the law enforcement or
8 intelligence authorities of any agency.

9 “(f) DEFINITIONS.—In this section:

10 “(1) The term ‘Federal systems’ means all in-
11 formation systems owned, operated, leased, or other-
12 wise controlled by an agency, or on behalf of an
13 agency, except for national security systems or those
14 information systems under the control of the De-
15 partment of Defense

16 “(2) The term ‘critical infrastructure informa-
17 tion systems’ means any physical or virtual informa-
18 tion system, no matter where such system exists,
19 that controls, processes, transmits, receives, or
20 stores electronic information in any form, including
21 data, voice, or video, that is—

22 “(A) vital to the functioning of critical in-
23 frastructure; or

24 “(B) owned or operated by or on behalf of
25 a State or local government entity.

1 **“SEC. 227. IDENTIFICATION OF SECTOR SPECIFIC CYBER-**
2 **SECURITY RISKS.**

3 “(a) IN GENERAL.—The Secretary, in coordination
4 with the head of the sector specific agency with responsi-
5 bility for critical infrastructure and the head of any Fed-
6 eral agency that is not a sector specific agency with re-
7 sponsibilities for regulating the critical infrastructure, and
8 in consultation with any private sector entity determined
9 appropriate by the Secretary, including the owners and op-
10 erators of critical infrastructure, shall, on a continuous
11 and sector-by-sector basis, identify and evaluate cyberse-
12 curity risks to critical infrastructure.

13 “(b) EVALUATION OF RISKS.—The Secretary shall
14 evaluate the cybersecurity risks identified under sub-
15 section (a) by taking into account each of the following:

16 “(1) The actual or assessed threat, including a
17 consideration of adversary capabilities and intent,
18 preparedness, target attractiveness, and deterrence
19 capabilities.

20 “(2) The extent and likelihood of death, injury,
21 or serious adverse effects to human health and safe-
22 ty caused by a disruption, destruction, or unauthor-
23 ized use of covered critical infrastructure.

24 “(3) The threat to national security caused by
25 the disruption, destruction or unauthorized use of
26 covered critical infrastructure.

1 “(4) The harm to the economy that would re-
2 sult from the disruption, destruction, or unauthor-
3 ized use of covered critical infrastructure.

4 “(5) Other risk-based security factors that the
5 Secretary, in consultation with the head of the sec-
6 tor specific agency with responsibility for covered
7 critical infrastructure and the head of any Federal
8 agency that is not a sector specific agency with re-
9 sponsibilities for regulating covered critical infra-
10 structure, and in consultation with any private sec-
11 tor entity determined appropriate by the Secretary
12 to protect public health and safety, critical infra-
13 structure, or national and economic security.

14 “(c) AVAILABILITY OF IDENTIFIED RISKS.—The Sec-
15 retary shall ensure that the risks identified and evaluated
16 under this section for each sector and subsector are made
17 available to the owners and operators of critical infrastruc-
18 ture within each sector and subsector.

19 “(d) CATALOGUE OF RISK-BASED PERFORMANCE
20 STANDARDS.—

21 “(1) ESTABLISHMENT.—The Secretary shall es-
22 tablish a catalogue of existing internationally recog-
23 nized consensus-developed risk-based performance
24 standards, including such standards developed by
25 the National Institute of Standards and Technology.

1 Such catalogue shall include, for each such risk-
2 based performance standard, an analysis of each of
3 the following:

4 “(A) How well the performance standard
5 addresses the identified risks.

6 “(B) How cost-effective the implementa-
7 tion of the performance standard can be.

8 “(2) USE OF CATALOGUE.—The Secretary, in
9 conjunction with the heads of other appropriate
10 agencies, shall develop market-based incentives de-
11 signed to encourage the use of the catalogue estab-
12 lished under paragraph (1).

13 “(3) INCLUSION IN REGULATORY REGIMES.—
14 The Secretary, in coordination with the heads of sec-
15 tor specific agencies with responsibility for covered
16 critical infrastructure and the head of any Federal
17 agency that is not a sector specific agency with re-
18 sponsibilities for regulating covered critical infra-
19 structure, and in consultation with any private sec-
20 tor entity determined appropriate by the Secretary,
21 shall work to include the risk-based performance
22 standards identified in the catalogue established
23 under paragraph (1) in the regulatory regimes appli-
24 cable to covered critical infrastructure.

1 “(e) MITIGATION OF RISKS.—If the Secretary deter-
2 mines that no existing internationally-recognized risk-
3 based performance standard mitigates a risk identified
4 under subsection (a), the Secretary shall—

5 “(1) work with owners and operators of critical
6 infrastructure and suppliers of technology to appro-
7 priately mitigate the identified risk, including deter-
8 mining appropriate market-based incentives for de-
9 velopment and implementation of the identified miti-
10 gation; and

11 “(2) engage with appropriate international con-
12 sensus bodies to develop and strengthen standards
13 and practices to address the identified risk.

14 “(f) COVERED CRITICAL INFRASTRUCTURE DE-
15 FINED.—In this section, the term ‘covered critical infra-
16 structure’ means any facility or function that, by way of
17 cyber vulnerability, the destruction or disruption of or un-
18 authorized access to could result in—

19 [“(1) the loss of thousands of lives;]

20 [“(2) a major economic disruption, including—

21]

22 [“(A) the immediate failure of, or loss of
23 confidence in, a major financial market; or]

24 [“(B) the sustained disruption of financial
25 systems that would lead to long term cata-

1 strophic economic damage to the United
2 States;】

3 【“(3) mass evacuations of a major population
4 center for longer than 30 days; or】

5 【“(4) severe degradation of national security or
6 national security capabilities, including intelligence
7 and defense functions, but excluding military facili-
8 ties.】

9 **“SEC. 228. INFORMATION SHARING.**

10 “(a) INFORMATION SHARING.—The Secretary shall,
11 to the maximum extent possible, consistent with rules for
12 the handling of classified and sensitive but unclassified in-
13 formation, share relevant information regarding cyberse-
14 curity threats and vulnerabilities, and any proposed ac-
15 tions to mitigate them, with all Federal agencies, appro-
16 priate State or local government representatives, and ap-
17 propriate critical infrastructure information systems own-
18 ers and operators, including by expediting necessary secu-
19 rity clearances for designated points of contact for critical
20 infrastructure information systems.

21 “(b) PROTECTION OF INFORMATION.—The Secretary
22 shall designate, as appropriate, information received from
23 Federal agencies and from critical infrastructure informa-
24 tion systems owners and operators and information pro-
25 vided to Federal agencies or critical infrastructure infor-

1 mation systems owners and operators pursuant to this sec-
2 tion as sensitive security information and shall require and
3 enforce sensitive security information requirements for
4 handling, storage, and dissemination of any such informa-
5 tion.

6 **“SEC. 229. CYBERSECURITY RESEARCH AND DEVELOP-**
7 **MENT.**

8 “(a) IN GENERAL.—The Under Secretary for Science
9 and Technology shall support research, development, test-
10 ing, evaluation, and transition of cybersecurity technology,
11 including fundamental, long-term research to improve the
12 ability of the United States to prevent, protect against,
13 detect, respond to, and recover from acts of terrorism and
14 cyber attacks, with an emphasis on research and develop-
15 ment relevant to attacks that would cause a debilitating
16 impact on national security, national economic security,
17 or national public health and safety.

18 “(b) ACTIVITIES.—The research and development
19 testing, evaluation, and transition supported under sub-
20 section (a) shall include work to—

21 “(1) advance the development and accelerate
22 the deployment of more secure versions of funda-
23 mental Internet protocols and architectures, includ-
24 ing for the domain name system and routing proto-
25 cols;

1 “(2) improve and create technologies for detect-
2 ing attacks or intrusions, including real-time moni-
3 toring and real-time analytic technologies;

4 “(3) improve and create mitigation and recov-
5 ery methodologies, including techniques and policies
6 for real-time containment of attacks and develop-
7 ment of resilient networks and systems;

8 “(4) develop and support infrastructure and
9 tools to support cybersecurity research and develop-
10 ment efforts, including modeling, test beds, and data
11 sets for assessment of new cybersecurity tech-
12 nologies;

13 “(5) assist in the development and support of
14 technologies to reduce vulnerabilities in process con-
15 trol systems;

16 “(6) develop and support cyber forensics and
17 attack attribution; and

18 “(7) test, evaluate, and facilitate the transfer of
19 technologies associated with the engineering of less
20 vulnerable software and securing the information
21 technology software development lifecycle.

22 “(c) COORDINATION.—In carrying out this section,
23 the Under Secretary shall coordinate activities with—

24 “(1) the Assistant Secretary for Infrastructure
25 Protection; and

1 “(2) the heads of other relevant Federal depart-
2 ments and agencies, including the National Science
3 Foundation, the Defense Advanced Research
4 Projects Agency, the Information Assurance Direc-
5 torate of the National Security Agency, the National
6 Institute of Standards and Technology, the Depart-
7 ment of Commerce, and other appropriate working
8 groups established by the President to identify
9 unmet needs and cooperatively support activities, as
10 appropriate.

11 **“SEC. 230. PERSONNEL AUTHORITIES RELATED TO THE OF-**
12 **FICE OF CYBERSECURITY AND COMMUNICA-**
13 **TIONS.**

14 “(a) IN GENERAL.— In order to assure that the De-
15 partment has the necessary resources to carry out the mis-
16 sion of securing Federal systems and critical infrastruc-
17 ture information systems, the Secretary may, as nec-
18 essary, convert competitive service positions, and the in-
19 cumbents of such positions, within the Office of Cyberse-
20 curity and Communications to excepted service, or may
21 establish new positions within the Office of Cybersecurity
22 and Communications in the excepted service, to the extent
23 that the Secretary determines such positions are necessary
24 to carry out the cybersecurity functions of the Depart-
25 ment.

1 “(b) COMPENSATION.—The Secretary may—

2 “(1) fix the compensation of individuals who
3 serve in positions referred to in subsection (a) in re-
4 lation to the rates of pay provided for comparable
5 positions in the Department and subject to the same
6 limitations on maximum rates of pay established for
7 employees of the Department by law or regulations;
8 and

9 “(2) provide additional forms of compensation,
10 including benefits, incentives, and allowances, that
11 are consistent with and not in excess of the level au-
12 thORIZED for comparable positions authorized under
13 title 5, United States Code.

14 “(c) RETENTION BONUSES.—Notwithstanding any
15 other provision of law, the Secretary may pay a retention
16 bonus to any employee appointed under this section, if the
17 Secretary determines that the bonus is needed to retain
18 essential personnel. Before announcing the payment of a
19 bonus under this subsection, the Secretary shall submit
20 a written explanation of such determination to the Com-
21 mittee on Homeland Security of the House of Representa-
22 tives and the Committee on Homeland Security and Gov-
23 ernmental Affairs of the Senate.

24 “(d) ANNUAL REPORT.—Not later than one year
25 after the date of the enactment of this section, and annu-

1 ally thereafter, the Secretary shall submit to the Com-
2 mittee on Homeland Security of the House of Representa-
3 tives and the Committee on Homeland Security and Gov-
4 ernment Affairs of the Senate a detailed report that in-
5 cludes, for the period covered by the report—

6 “(1) a discussion the Secretary’s use of the
7 flexible authority authorized under this section to re-
8 cruit and retain qualified employees;

9 “(2) metrics on relevant personnel actions, in-
10 cluding—

11 “(A) the number of qualified employees
12 hired by occupation and grade, level, or pay
13 band;

14 “(B) the total number of veterans hired;

15 “(C) the number of separations of qualified
16 employees;

17 “(D) the number of retirements of quali-
18 fied employees; and

19 “(E) the number and amounts of recruit-
20 ment, relocation, and retention incentives paid
21 to qualified employees by occupation and grade.
22 level, or pay band; and

23 “(3) long-term and short-term strategic goals to
24 address critical skills deficiencies, including an anal-
25 ysis of the numbers of and reasons for attrition of

1 employees and barriers to recruiting and hiring indi-
2 viduals qualified in cybersecurity.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 2(b) of such Act is amended by inserting after
5 the item relating to section 225 the following new items:

“Sec. 226. National cybersecurity authority.

“Sec. 227. Voluntary private sector information security standards.

“Sec. 228. Information sharing.

“Sec. 229. Cybersecurity research and development.

“Sec. 230. Personnel authorities related to the Office of Cybersecurity and
Communications.”.

6 (c) PLAN FOR EXECUTION OF AUTHORITIES.—Not
7 later than 120 days after the date of the enactment of
8 this Act, the Secretary of Homeland Security shall submit
9 to the Committee on Homeland Security of the House of
10 Representatives and the Committee on Homeland Security
11 and Governmental Affairs of the Senate a report con-
12 taining a plan for the execution of the authorities con-
13 tained in the amendment made by subsection (a).

14 **SEC. 3. NATIONAL INFORMATION SHARING ORGANIZATION.**

15 (a) NATIONAL INFORMATION SHARING ORGANIZA-
16 TION.—

17 (1) IN GENERAL.—Title II of the Homeland Se-
18 curity Act of 2002, as amended by section 2, is fur-
19 ther amended by adding at the end the following:

1 **“Subtitle E—National Information**
2 **Sharing Organization**

3 **“SEC. 241. ESTABLISHMENT OF NATIONAL INFORMATION**
4 **SHARING ORGANIZATION.**

5 “(a) ESTABLISHMENT.—There is established a not-
6 for-profit organization for sharing cyber threat informa-
7 tion and exchanging technical assistance, advice, and sup-
8 port and developing and disseminating necessary informa-
9 tion security technology. Such organization shall be des-
10 ignated as the ‘National Information Sharing Organiza-
11 tion’.

12 “(b) PURPOSE.—The National Information Sharing
13 Organization shall serve as a national clearinghouse for
14 the exchange of cyber threat information so that the own-
15 ers and operators of networks or systems in the private
16 sector, educational institutions, State, tribal, and local
17 governments, entities operating critical infrastructure, and
18 the Federal Government have access to timely and action-
19 able information in order to protect their networks or sys-
20 tems as effectively as possible.

21 “(c) DESIGNATION.—Not later than 120 days after
22 the date of the enactment of this subtitle, the board of
23 directors established in section 243 shall designate the ap-
24 propriate organization or organizations as the National
25 Information Sharing Organization.

1 “(d) CRITERIA FOR DESIGNATION.—The board of di-
2 rectors shall select organizations to function as the Na-
3 tional Information Sharing Organization using the fol-
4 lowing criteria:

5 “(1) Whether the organization has received rec-
6 ognition from the Secretary of Homeland Security
7 for its cyber capabilities.

8 “(2) Whether the organization has dem-
9 onstrated the ability to address cyber-related issues
10 in a trusted and cooperative environment maxi-
11 mizing public-private partnerships.

12 “(3) Whether the organization has dem-
13 onstrated the capability to deploy cybersecurity serv-
14 ices for the detection, prevention, and mitigation of
15 cyber-related issues.

16 “(4) Whether the organization has an oper-
17 ational center that is open 24 hours a day, seven
18 days a week, and is capable of determining, ana-
19 lyzing, and responding to cyber events.

20 “(5) Whether the organization has a proven re-
21 lationship with the private sector critical infrastruc-
22 ture sectors.

23 **“SEC. 242. MISSION AND ACTIVITIES.**

24 “The National Information Sharing Organization
25 shall—

1 “(1) facilitate the exchange of information and
2 technical assistance and support related to the secu-
3 rity of public, private, and critical infrastructure in-
4 formation networks, including by—

5 “(A) ensuring that the information ex-
6 changed shall be stripped of all information
7 identifying the submitter and shall be available
8 to members of the National Information Shar-
9 ing Organization, including Federal, State, and
10 local government agencies; and

11 “(B) sharing timely and actionable threat
12 and vulnerability information originating
13 through intelligence collection with appro-
14 priately cleared members of the National Infor-
15 mation Sharing Organization;

16 “(2) create a common operating picture by
17 combining agreed upon network and cyber threat
18 warning information to be shared—

19 “(A) through a secure automated mecha-
20 nism to be determined by the board; and

21 “(B) with designated members of the Na-
22 tional Information Sharing Organization, in-
23 cluding the Federal Government;

24 “(3) undertake collaborative research and devel-
25 opment projects to improve the level of cybersecurity

1 in critical infrastructure information systems while
2 maintaining impartiality, the independence of mem-
3 bers of the National Information Sharing Organiza-
4 tion, and vendor neutrality;

5 “(4) develop language to be incorporated into
6 the membership agreement regarding the transfer-
7 ability and use of intellectual property developed by
8 the National Information Sharing Organization and
9 its members under this subtitle; and

10 “(5) integrate with the Federal Government
11 through the National Cybersecurity and Communica-
12 tions Integration Center and other existing informa-
13 tion sharing and analysis centers, as appropriate.

14 **“SEC. 243. BOARD OF DIRECTORS.**

15 “(a) IN GENERAL.—The National Information Shar-
16 ing Organization shall have a board of directors which
17 shall be responsible for—

18 “(1) the executive and administrative operation
19 of the National Information Sharing Organization,
20 including matters relating to funding and promotion
21 of the National Information Sharing Organization;
22 and

23 “(2) ensuring and facilitating compliance by
24 members of the National Information Sharing Orga-
25 nization with the requirements of this subtitle.

1 “(b) COMPOSITION.—The board shall be composed of
2 the following members:

3 “(1) One representative from the Department
4 of Homeland Security.

5 “(2) Four representatives from three different
6 Federal agencies with significant responsibility for
7 cybersecurity.

8 “(3) Ten representatives from the private sec-
9 tor, including at least one member representing a
10 small business interest and members representing
11 each of the following critical infrastructure sectors
12 and subsectors:

13 “(A) Banking and finance.

14 “(B) Communications.

15 “(C) Defense industrial base.

16 “(D) Energy, electricity subsector.

17 “(E) Energy, oil, and natural gas.

18 “(F) Health care and public health.

19 “(G) Information technology.

20 “(4) Two representatives from the privacy and
21 civil liberties community.

22 “(c) INITIAL APPOINTMENT.—Not later than 30 days
23 after the date of the enactment of this subtitle, the Sec-
24 retary of Homeland Security, in consultation with the
25 heads of the sector specific agencies of the sectors and

1 subsectors referred to in subsection (b)(3), shall appoint
2 the members of the board described under subsection
3 (b)(3) from individuals identified by the sector coordi-
4 nating councils of sectors and subsectors referred to in
5 subsection (b)(3).

6 “(d) TERMS.—

7 “(1) REPRESENTATIVES OF CERTAIN FEDERAL
8 AGENCIES.—Each member of the board described in
9 subsection (b) shall serve for a term that is not
10 longer than three years from the date of the mem-
11 ber’s appointment.

12 “(2) OTHER REPRESENTATIVES.—The original
13 private sector members of the board described sub-
14 section (b) shall serve an initial term of one year
15 from the date of appointment under subsection (c),
16 at which time the members of the National Informa-
17 tion Sharing Organization shall conduct elections in
18 accordance with the procedures established under
19 subsection (e).

20 “(e) RULES AND PROCEDURES.—Not later than 90
21 days after the date of the enactment of this Act, the board
22 shall establish rules and procedures for the election and
23 service of members of the board described in paragraphs
24 (3) and (4) of subsection (b).

1 “(f) LEADERSHIP.—The board shall elect from
2 among its members a chair and vice-chair of the board,
3 who shall serve under such terms and conditions as the
4 board may establish. The chair of the board may not be
5 a Federal employee.

6 “(g) SUB-BOARDS.—The board shall have the author-
7 ity to constitute such sub-boards, or other advisory groups
8 or panels, as may be necessary to assist the board in car-
9 rying out its functions under this section.

10 **“SEC. 244. CHARTER.**

11 “The board shall develop a charter to govern the op-
12 erations and administration of the National Information
13 Sharing Organization. The charter shall cover each of the
14 following:

15 “(1) The organizational structure of the Na-
16 tional Information Sharing Organization.

17 “(2) The governance of the National Informa-
18 tion Sharing Organization.

19 “(3) A mission statement of the National Infor-
20 mation Sharing Organization.

21 “(4) Criteria for membership of the National
22 Information Sharing Organization and for termi-
23 nation of such membership.

1 “(5) A funding model of the National Informa-
2 tion Sharing Organization, including costs, if any,
3 for membership.

4 “(6) Rules for sharing information with mem-
5 bers of the National Information Sharing Organiza-
6 tion, including the treatment and ownership of intel-
7 lectual property provided by or to the National In-
8 formation Sharing Organization, limitations on li-
9 ability, and consideration of any necessary measures
10 to mitigate anti-trust concerns;

11 “(7) Technical requirements for participation in
12 the common operating picture and a technical archi-
13 tecture that enables an automated, real-time sharing
14 among members and Federal Government agencies.

15 “(8) Rules for participating in collaborative re-
16 search and development projects.

17 “(9) Protections of privacy and civil liberties to
18 be used by the National Information Sharing Orga-
19 nization and its members, including appropriate
20 measures for public transparency and oversight.

21 “(10) Security requirements and member obli-
22 gations for the protection of information from other
23 sources, including private and governmental.

1 **“SEC. 245. MEMBERSHIP.**

2 “(a) REQUIREMENT FOR PROCEDURES.—Not later
3 than 90 days after the date of the enactment of this sub-
4 title, the board of directors of the National Information
5 Sharing Organization shall establish criteria procedures
6 for the voluntary membership by State and local govern-
7 ment departments, agencies, and entities, private sector
8 businesses and organizations, and academic institutions in
9 the National Information Sharing Organization.

10 “(b) PARTICIPATION BY FEDERAL AGENCIES.—The
11 Secretary of Homeland Security, in coordination with the
12 Secretary of Energy, the Director of National Intelligence,
13 the Secretary of Defense, the Director of the Federal Bu-
14 reau of Investigation, and the heads of other appropriate
15 Federal agencies, shall provide for the participation and
16 cooperation of such Federal agencies in the National In-
17 formation Sharing Organization.

18 **“SEC. 246. FUNDING.**

19 “(a) IN GENERAL.—Except as provided in subsection
20 (b), annual administrative and operational expenses for
21 the National Information Sharing Organization shall be
22 paid by the members of such Organization, as determined
23 by the board of directors of the Organization.

24 “(b) MAXIMUM FEDERAL CONTRIBUTION.—Not
25 more than 15 percent of the annual expenses referred to
26 in subsection (a) may be paid by the Federal Government.

1 Such amount shall be provided under the direction of the
2 Secretary of Homeland Security and shall be included
3 within the cybersecurity program budget request for the
4 Department of Homeland Security.

5 **“SEC. 247. CLASSIFIED INFORMATION.**

6 “Consistent with the protection of sensitive intel-
7 ligence sources and methods, the Secretary, in conjunction
8 with the Director of National Intelligence, shall facili-
9 tate—

10 “(1) the sharing of classified information in the
11 possession of a Federal agency related to threats to
12 information networks with cleared members of the
13 National Information Sharing Organization, includ-
14 ing representatives of the private sector and of pub-
15 lic and private sector entities operating critical infra-
16 structure; and

17 “(2) the declassification and sharing of infor-
18 mation in the possession of a Federal agency related
19 to threats to information networks with members of
20 the National Information Sharing Organization.

21 **“SEC. 248. VOLUNTARY INFORMATION SHARING.**

22 “(a) **USES OF SHARED INFORMATION.**—Notwith-
23 standing any other provision of law, information shared
24 with or provided to the National Information Sharing Or-
25 ganization or to a Federal agency through the National

1 Information Sharing Organization by any member of the
2 National Information Sharing Organization that is not a
3 Federal agency in furtherance of the mission and activities
4 of the National Information Sharing Organization as de-
5 scribed in section 242—

6 “(1) shall be exempt from disclosure under sec-
7 tion 552 of title 5, United States Code (commonly
8 referred to as the Freedom of Information Act);

9 “(2) shall not, without the written consent of
10 the person or entity submitting such information, be
11 used directly by any Federal agency, any other Fed-
12 eral, State, tribal, or local authority, or any third
13 party, in any civil action arising under Federal or
14 State law if such information is submitted to the
15 National Information Sharing Organization for the
16 purpose of facilitating the missions of such Organi-
17 zation, as articulated in the mission statement re-
18 quired under section 244;

19 “(3) shall not, without the written consent of
20 the person or entity submitting such information, be
21 used or disclosed by any officer or employee of the
22 United States for purposes other than the purposes
23 of this title, except—

24 “(A) to further an investigation or the
25 prosecution of a criminal act; or

1 “(B) to disclose the information to the ap-
2 propriate congressional committee;

3 “(4) shall not, if subsequently provided to a
4 State or local government or government agency—

5 “(A) be made available pursuant to any
6 State or local law requiring disclosure of infor-
7 mation or records;

8 “(B) otherwise be disclosed or distributed
9 to any party by such State or local government
10 or government agency without the written con-
11 sent of the person or entity submitting such in-
12 formation; or

13 “(C) be used other than for the purpose of
14 protecting information systems, or in further-
15 ance of an investigation or the prosecution of a
16 criminal act; and

17 “(5) does not constitute a waiver of any appli-
18 cable privilege or protection provided under law,
19 such as information that is proprietary, business
20 sensitive, relates specifically to the submitting per-
21 son or entity, or is otherwise not appropriately in
22 the public domain.

23 “(b) LIMITATION.—The Federal Advisory Committee
24 Act (5 U.S.C. App.) shall not apply to any communication

1 of information to a Federal agency made pursuant to this
2 title.

3 “(c) PROCEDURES.—

4 “(1) IN GENERAL.—Not later than 90 days
5 after the date of the enactment of this subtitle, the
6 board of directors of the National Information Shar-
7 ing Organization shall establish uniform procedures
8 for the receipt, care, and storage of information that
9 is voluntarily submitted to the Federal Government
10 through the National Information Sharing Organiza-
11 tion.

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

14 “(A) the acknowledgment of receipt by the
15 National Information Sharing Organization of
16 cyber threat information that is voluntarily sub-
17 mitted to the National Information Sharing Or-
18 ganization;

19 “(B) the maintenance of the identification
20 of such information;

21 “(C) the care and storage of such informa-
22 tion;

23 “(D) limiting subsequent dissemination of
24 such information to ensure that such informa-
25 tion is not used for an unauthorized purpose;

1 “(E) the protection of the privacy rights
2 and civil liberties of any individuals who are
3 subjects of such information; and

4 “(F) the protection and maintenance of
5 the confidentiality of such information so as to
6 permit the sharing of such information within
7 the Federal Government and with State, tribal,
8 and local governments, and the issuance of no-
9 tices and warnings related to the protection of
10 information networks, in such manner as to
11 protect from public disclosure the identity of
12 the submitting person or entity, or information
13 that is proprietary, business sensitive, relates
14 specifically to the submitting person or entity,
15 and is otherwise not appropriately in the public
16 domain.

17 “(d) INDEPENDENTLY OBTAINED INFORMATION.—
18 Nothing in this section shall be construed to limit or other-
19 wise affect the ability of a Federal agency, a State, tribal,
20 or local government or government agency, or any third
21 party—

22 “(1) to obtain or disseminate cyber threat infor-
23 mation in a manner other than through the National
24 Information Sharing Organization; and

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

3 **["SEC. 249. PENALTIES.**

4 **["(a) IN GENERAL.—**It shall be unlawful for any of-
5 ficer or employee of the United States or of any Federal
6 agency to knowingly publish, divulge, disclose, or make
7 known in any manner or to any extent not authorized by
8 law, any cyber threat information protected from disclo-
9 sure by this title coming to such officer or employee in
10 the course of the employee’s employment or official duties
11 or by reason of any examination or investigation made by,
12 or return, report, or record made to or filed with, such
13 officer, employee, or agency.】

14 **["(b) PENALTY.—**Any person who violates sub-
15 section (a) shall be fined under title 18, United States
16 Code, imprisoned for not more than one year, or both, and
17 shall be removed from office or employment.】

18 **“SEC. 250. AUTHORITY TO ISSUE WARNINGS.**

19 “The Secretary may provide advisories, alerts, and
20 warnings to relevant companies, targeted sectors, other
21 government entities, or the general public regarding poten-
22 tial threats to information networks as appropriate. In
23 issuing such an advisory, alert, or warning, the Secretary
24 shall take appropriate actions to protect from disclosure—

1 “(1) the source of any voluntarily submitted in-
2 formation that forms the basis for the advisory,
3 alert, or warning; and

4 “(2) information that is proprietary, business
5 sensitive, relates specifically to the submitting per-
6 son or entity, or is otherwise not appropriate for dis-
7 closure in the public domain.

8 **["SEC. 251. EXEMPTION FROM ANTITRUST PROHIBITIONS.**

9 “The exchange of information by and between private
10 sector members of the National Information Sharing Or-
11 ganization in furtherance of the mission and activities of
12 the National Information Sharing Organization shall not
13 be considered a violation of any provision of the antitrust
14 laws (as such term is defined in the first section of the
15 Clayton Act (15 U.S.C. 12)).”

16 **“SEC. 252. LIMITATION.**

17 “For any fiscal year after fiscal year 2015, the
18 amount authorized to be appropriated for the National In-
19 formation Sharing Organization may not exceed the
20 amount provided by the largest private sector member of
21 the National Information Sharing Organization for that
22 fiscal year.”

23 (2) CLERICAL AMENDMENT.—The table of con-
24 tents in section 2(b) of such Act, as amended by sec-

1 tion 2, is further amended by adding at the end of
2 the items relating to title II the following new items:

“Subtitle E—National Information Sharing Organization

“Sec. 241. Establishment of National Information Sharing Organization.

“Sec. 242. Mission and activities.

“Sec. 243. Board of directors.

“Sec. 244. Charter.

“Sec. 245. Membership.

“Sec. 246. Funding.

“Sec. 247. Classified information.

“Sec. 248. Voluntary information sharing.

“Sec. 249. Penalties.

“Sec. 250. Authority to issue warnings.

“Sec. 251. Exemption from antitrust prohibitions.

“Sec. 252. Limitation.”.

3 (b) INITIAL EXPENSES.—There is authorized to be
4 appropriated \$_____ for initial ex-
5 penses associated with the establishment of the National
6 Information Sharing Organization under subtitle E of title
7 II of the Homeland Security Act of 2002, as added by
8 subsection (a).