

112TH CONGRESS
1ST SESSION

H. R. 3674

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

DECEMBER 15, 2011

Mr. DANIEL E. LUNGREN of California (for himself, Mr. KING of New York, Mr. McCAUL, Mr. BILIRAKIS, Mrs. MILLER of Michigan, Mr. WALBERG, Mr. MARINO, Mr. LONG, Mr. TURNER of New York, Mr. STIVERS, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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 “Promoting and En-
5 hancing Cybersecurity and Information Sharing Effective-
6 ness Act of 2011” or the “PRECISE 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 and subject to
14 the availability of resources, critical infrastructure
15 information systems in consultation with the heads
16 of other agencies or governmental and private enti-
17 ties that own and operate such systems, that may
18 include threat, vulnerability, and impact assessments
19 and penetration testing, or other comprehensive as-
20 sessments techniques;

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

1 preprehensive protective capabilities and other techno-
2 logical solutions;

3 “(3) acquire, integrate, and facilitate the adop-
4 tion of new cybersecurity technologies and practices
5 in a technologically and vendor-neutral manner to
6 keep pace with emerging terrorist and other cyberse-
7 curity threats and developments, including through
8 research and development, technical service agree-
9 ments, and making such technologies available to
10 governmental and private entities that own or oper-
11 ate critical infrastructure information systems, as
12 necessary to accomplish the purpose of this section;

13 “(4) maintain the capability to serve as a focal
14 point with the Federal Government for cybersecu-
15 rity, responsible for—

16 “(A) the coordination of the protection of
17 Federal systems and critical infrastructure in-
18 formation systems;

19 “(B) the coordination of national cyber in-
20 cident response;

21 “(C) facilitating information sharing, inter-
22 actions, and collaborations among and between
23 Federal agencies, State and local governments,
24 the private sector, academia, and international
25 partners;

1 “(D) working with appropriate Federal
2 agencies, State and local governments, the pri-
3 vate sector, academia, and international part-
4 ners to prevent and respond to terrorist and
5 other cybersecurity threats and incidents involv-
6 ing Federal systems and critical infrastructure
7 information systems pursuant to the national
8 cyber incident response plan and supporting
9 plans developed in accordance with paragraph
10 (8);

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

19 “(F) the integration of information from
20 Federal Government and non-federal network
21 operation centers and security operations cen-
22 ters;

23 “(G) the compilation and analysis of infor-
24 mation about risks and incidents regarding ter-
25 rorism or other causes that threaten Federal

1 systems and critical infrastructure information
2 systems;

3 “(H) the provision of incident prediction,
4 detection, analysis, mitigation, and response in-
5 formation and remote or on-site technical as-
6 sistance to heads of Federal agencies and, upon
7 request, governmental and private entities that
8 own or operate critical infrastructure; and

9 “(I) acting as the Federal Government
10 representative with the organization or organi-
11 zations designated under section 241;

12 “(5) assist in national efforts to mitigate com-
13 munications and information technology supply
14 chain vulnerabilities to enhance the security and the
15 resiliency of Federal systems and critical infrastruc-
16 ture information systems;

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

19 “(A) the importance of cybersecurity and
20 cyber ethics;

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

23 “(C) training opportunities to support the
24 development of an effective national cybersecu-

1 rity workforce and educational paths to cyberse-
2 curity professions;

3 “(7) establish, in coordination with the Director
4 of the National Institute of Standards and Tech-
5 nology and the heads of other appropriate agencies,
6 benchmarks and guidelines for making critical infra-
7 structure information systems more secure at a fun-
8 damental level, including through automation, inter-
9 operability, and privacy-enhancing authentication;

10 “(8) develop a national cybersecurity incident
11 response plan and supporting cyber incident re-
12 sponse and restoration plans, in consultation with
13 the heads of other relevant Federal agencies, owners
14 and operators of critical infrastructure, sector co-
15 ordinating councils, State and local governments,
16 and relevant non-governmental organizations and
17 based on applicable law that describe the specific
18 roles and responsibilities of governmental and pri-
19 vate entities during cyber incidents to ensure essen-
20 tial government operations continue;

21 “(9) develop and conduct exercises, simulations,
22 and other activities designed to support the national
23 response to terrorism and other cybersecurity
24 threats and incidents and evaluate the national

1 cyber incident response plan and supporting plans
2 developed in accordance with paragraph (8);

3 “(10) ensure that the technology and tools used
4 to accomplish the requirements of this section are
5 scientifically and operationally validated; and

6 “(11) take such other lawful action as may be
7 necessary and appropriate to accomplish the require-
8 ments of this section.

9 “(b) COORDINATION.—

10 “(1) COORDINATION WITH OTHER ENTITIES.—

11 In carrying out the cybersecurity activities under
12 this section, the Secretary shall coordinate, as ap-
13 propriate, with—

14 “(A) the head of any relevant agency or
15 entity;

16 “(B) representatives of State and local
17 governments;

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

20 “(D) suppliers of technology for critical in-
21 frastructure;

22 “(E) academia; and

23 “(F) international organizations and for-
24 eign partners.

1 “(2) COORDINATION OF AGENCY ACTIVITIES.—

2 The Secretary shall coordinate the activities under-
3 taken by agencies to protect Federal systems and
4 critical infrastructure information systems and pre-
5 pare the Nation to predict, anticipate, recognize, re-
6 spond to, recover from, and mitigate against risk of
7 acts of terrorism and other incidents involving such
8 systems and infrastructure.

9 “(3) LEAD CYBERSECURITY OFFICIAL.—The

10 Secretary shall designate a lead cybersecurity official
11 to provide leadership to the cybersecurity activities
12 of the Department and to ensure that the Depart-
13 ment’s cybersecurity activities under this subtitle are
14 coordinated with all other infrastructure protection
15 and cyber-related programs and activities of the De-
16 partment, including those of any intelligence or law
17 enforcement components or entities within the De-
18 partment.

19 “(4) REPORTS TO CONGRESS.—The lead cyber-

20 security official shall make regular reports to the ap-
21 propriate committees of Congress on the coordina-
22 tion of cyber-related programs across the Depart-
23 ment.

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

4 “(1) articulates the actions necessary to assure
5 the readiness, reliability, continuity, integrity, and
6 resilience of Federal systems and critical infrastruc-
7 ture information systems;

8 “(2) is informed by the need to maintain eco-
9 nomic prosperity and facilitate market leadership for
10 the United States information and communications
11 industry; and

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

14 “(d) ACCESS TO INFORMATION.—The Secretary shall
15 ensure that the organization or organizations designated
16 under section 241 have full and timely access to properly
17 anonymized cyber incident information originating within
18 the Federal civilian networks to populate the common op-
19 erating picture described in section 242.

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

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

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

8 “(g) DEFINITIONS.—In this section:

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

15 “(2) The term ‘critical infrastructure informa-
16 tion systems’ means any physical or virtual informa-
17 tion system that controls, processes, transmits, re-
18 ceives, or stores electronic information in any form,
19 including data, voice, or video, that is—

20 “(A) vital to the functioning of critical in-
21 frastructure as defined in section 5195c(e) of
22 title 42; or

23 “(B) owned or operated by or on behalf of
24 a State or local government entity that is nec-

1 essary to ensure essential government oper-
2 ations continue.

3 **“SEC. 227. IDENTIFICATION OF SECTOR SPECIFIC CYBER-**
4 **SECURITY RISKS.**

5 “(a) IN GENERAL.—The Secretary shall, on a contin-
6 uous and sector-by-sector basis, identify and evaluate cy-
7 bersecurity risks to critical infrastructure. In carrying out
8 this subsection, the Secretary shall coordinate, as appro-
9 priate, with the following:

10 “(1) The head of the sector specific agency with
11 responsibility for critical infrastructure.

12 “(2) The head of any agency with responsibil-
13 ities for regulating the critical infrastructure.

14 “(3) The owners and operators of critical infra-
15 structure and any private sector entity determined
16 appropriate by the Secretary.

17 “(b) EVALUATION OF RISKS.—The Secretary, in co-
18 ordination with the individuals and entities referred to in
19 subsection (a), shall evaluate the cybersecurity risks iden-
20 tified under subsection (a) by taking into account each of
21 the following:

22 “(1) The actual or assessed threat, including a
23 consideration of adversary capabilities and intent,
24 preparedness, target attractiveness, and deterrence
25 capabilities.

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

5 “(3) The threat to national security caused by
6 the disruption, destruction or unauthorized use of
7 critical infrastructure.

8 “(4) The harm to the economy that would re-
9 sult from the disruption, destruction, or unauthor-
10 ized use of critical infrastructure.

11 “(5) Other risk-based security factors that the
12 Secretary, in consultation with the head of the sec-
13 tor specific agency with responsibility for critical in-
14 frastructure and the head of any Federal agency
15 that is not a sector specific agency with responsibil-
16 ities for regulating critical infrastructure, and in
17 consultation with any private sector entity deter-
18 mined appropriate by the Secretary to protect public
19 health and safety, critical infrastructure, or national
20 and economic security.

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

1 “(d) COLLECTION OF RISK-BASED PERFORMANCE
2 STANDARDS.—

3 “(1) REVIEW AND ESTABLISHMENT.—The Sec-
4 retary, in coordination with the heads of other ap-
5 propriate agencies, shall review existing internation-
6 ally recognized consensus-developed risk-based per-
7 formance standards, including such standards devel-
8 oped by the National Institute of Standards and
9 Technology, for inclusion in a common collection.
10 Such collection shall include, for each such risk-
11 based performance standard, an analysis of each of
12 the following:

13 “(A) How well the performance standard
14 addresses the identified risks.

15 “(B) How cost-effective the standard im-
16 plementation of the performance standard can
17 be.

18 “(2) USE OF COLLECTION.—The Secretary, in
19 conjunction with the heads of other appropriate
20 agencies, shall develop market-based incentives de-
21 signed to encourage the use of the collection estab-
22 lished under paragraph (1).

23 “(3) INCLUSION IN REGULATORY REGIMES.—
24 The heads of sector specific agencies with responsi-
25 bility for covered critical infrastructure and the head

1 of any Federal agency that is not a sector specific
2 agency with responsibilities for regulating covered
3 critical infrastructure, in consultation with the Sec-
4 retary and with any private sector entity determined
5 appropriate by the Secretary, shall propose through
6 notice and comment rulemaking to include the most
7 effective and cost-efficient risk-based performance
8 standards identified in the collection established
9 under paragraph (1) in the regulatory regimes appli-
10 cable to covered critical infrastructure.

11 “(e) MITIGATION OF RISKS.—If the Secretary deter-
12 mines that no existing internationally-recognized risk-
13 based performance standard mitigates a risk identified
14 under subsection (a), the Secretary shall—

15 “(1) work with owners and operators of critical
16 infrastructure and suppliers of technology to appro-
17 priately mitigate the identified risk, including deter-
18 mining appropriate market-based incentives for de-
19 velopment and implementation of the identified miti-
20 gation; and

21 “(2) engage with the National Institute of
22 Standards and Technology and appropriate inter-
23 national consensus bodies that develop and strength-
24 en standards and practices to address the identified
25 risk.

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

6 “(1) a significant loss of life;

7 “(2) a major economic disruption, including—

8 “(A) the immediate failure of, or loss of
9 confidence in, a major financial market; or

10 “(B) the sustained disruption of financial
11 systems that would lead to long term cata-
12 strophic economic damage to the United States;

13 “(3) mass evacuations of a major population
14 center for an extended length of time; or

15 “(4) severe degradation of national security or
16 national security capabilities, including intelligence
17 and defense functions, but excluding military facili-
18 ties.

19 “(g) REDRESS.—

20 “(1) IN GENERAL.—Subject to paragraphs (2)
21 and (3), the Secretary shall develop a mechanism,
22 consistent with subchapter II of chapter 5 of title 5,
23 United States Code, for an owner or operator noti-
24 fied under subsection (f) to appeal the identification

1 of a facility or function as covered critical infrastruc-
2 ture under this section.

3 “(2) APPEAL TO FEDERAL COURT.—A civil ac-
4 tion seeking judicial review of a final agency action
5 taken under the mechanism developed under para-
6 graph (1) shall be filed in the United States District
7 Court for the District of Columbia.

8 “(3) COMPLIANCE.—The owner or operator of a
9 facility or function identified as covered critical in-
10 frastructure shall comply with any requirement of
11 this subtitle relating to covered critical infrastruc-
12 ture until such time as the facility or function is no
13 longer identified as covered critical infrastructure,
14 based on—

15 “(A) an appeal under paragraph (1);

16 “(B) a determination of the Secretary un-
17 related to an appeal; or

18 “(C) a final judgment entered in a civil ac-
19 tion seeking judicial review brought in accord-
20 ance with paragraph (2).

21 **“SEC. 228. INFORMATION SHARING.**

22 “(a) CYBERSECURITY INFORMATION.—The Secretary
23 shall be responsible for making all cyber threat informa-
24 tion, provided pursuant to section 202 of this title, avail-
25 able to appropriate owners and operators of critical infra-

1 structure on a timely basis consistent with the responsibil-
2 ities of the Secretary to provide information related to
3 threats to critical infrastructures to the organization des-
4 igned under section 241.

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

16 “(c) PROTECTION OF INFORMATION.—The Secretary
17 shall designate, as appropriate, information received from
18 Federal agencies and from critical infrastructure informa-
19 tion systems owners and operators and information pro-
20 vided to Federal agencies or critical infrastructure infor-
21 mation systems owners and operators pursuant to this sec-
22 tion as sensitive security information and shall require and
23 enforce sensitive security information requirements for
24 handling, storage, and dissemination of any such informa-

1 tion, including proper protections for personally identifi-
2 cable information.

3 **“SEC. 229. CYBERSECURITY RESEARCH AND DEVELOP-**
4 **MENT.**

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

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

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

23 “(2) improve, create, and advance the research
24 and development of techniques and technologies for

1 proactive detection and identification of threats, at-
2 tacks, and acts of terrorism before they occur;

3 “(3) advance technologies for detecting attacks
4 or intrusions, including real-time monitoring and
5 real-time analytic technologies;

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

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

15 “(6) assist in the development and support of
16 technologies to reduce vulnerabilities in process con-
17 trol systems;

18 “(7) develop and support cyber forensics and
19 attack attribution;

20 “(8) test, evaluate, and facilitate the transfer of
21 technologies associated with the engineering of less
22 vulnerable software and securing the information
23 technology software development lifecycle; and

24 “(9) ensure new cybersecurity technologies are
25 scientifically and operationally validated.

1 and Communications in the excepted service, to the extent
2 that the Secretary determines such positions are necessary
3 to carry out the cybersecurity functions of the Depart-
4 ment.

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

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

13 “(2) provide additional forms of compensation,
14 including benefits, incentives, and allowances, that
15 are consistent with and not in excess of the level au-
16 thorized for comparable positions authorized under
17 title 5, United States Code.

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

1 tives and the Committee on Homeland Security and Gov-
2 ernmental Affairs of the Senate.

3 “(d) ANNUAL REPORT.—Not later than one year
4 after the date of the enactment of this section, and annu-
5 ally thereafter, the Secretary shall submit to the Com-
6 mittee on Homeland Security of the House of Representa-
7 tives and the Committee on Homeland Security and Gov-
8 ernment Affairs of the Senate a detailed report that in-
9 cludes, for the period covered by the report—

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

13 “(2) metrics on relevant personnel actions, in-
14 cluding—

15 “(A) the number of qualified employees
16 hired by occupation and grade, level, or pay
17 band;

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

19 “(C) the number of separations of qualified
20 employees;

21 “(D) the number of retirements of quali-
22 fied employees; and

23 “(E) the number and amounts of recruit-
24 ment, relocation, and retention incentives paid

1 to qualified employees by occupation and grade,
2 level, or pay band; and

3 “(3) long-term and short-term strategic goals to
4 address critical skills deficiencies, including an anal-
5 ysis of the numbers of and reasons for attrition of
6 employees and barriers to recruiting and hiring indi-
7 viduals qualified in cybersecurity.”.

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

“Sec. 226. National cybersecurity authority.

“Sec. 227. Identification of sector specific cybersecurity risks.

“Sec. 228. Information sharing.

“Sec. 229. Cybersecurity research and development.

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

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

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

20 (a) NATIONAL INFORMATION SHARING ORGANIZA-
21 TION.—

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

4 **“Subtitle E—National Information**
5 **Sharing Organization**

6 **“SEC. 241. ESTABLISHMENT OF NATIONAL INFORMATION**
7 **SHARING ORGANIZATION.**

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

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

24 “(c) DESIGNATION.—Not later than 120 days after
25 the date of the enactment of this subtitle, the board of

1 directors established in section 243 shall designate the ap-
2 propriate organization or organizations as the National
3 Information Sharing Organization.

4 “(d) CRITERIA FOR DESIGNATION.—The board of di-
5 rectors shall select the organization or organizations to
6 function as the National Information Sharing Organiza-
7 tion by taking into consideration the following criteria and
8 other criteria found appropriate by the board:

9 “(1) Whether the organization or organizations
10 have received recognition from the Secretary of
11 Homeland Security for its cyber capabilities.

12 “(2) Whether the organization or organizations
13 have demonstrated the ability to address cyber-re-
14 lated issues in a trusted and cooperative environ-
15 ment maximizing public-private partnerships.

16 “(3) Whether the organization or organizations
17 have demonstrated the capability to deploy cyberse-
18 curity services for the detection, prevention, and
19 mitigation of cyber-related issues.

20 “(4) Whether the organization or organizations
21 have an operational center that is open 24 hours a
22 day, seven days a week, and is capable of deter-
23 mining, analyzing, and responding to cyber events.

1 “(5) Whether the organization or organizations
2 have a proven relationship with the private sector
3 critical infrastructure sectors.

4 “(6) Whether the organization or organizations
5 have experience implementing privacy protections to
6 safeguard, sensitive information, including person-
7 ally identifiable information, in transit and at rest.

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

9 “The National Information Sharing Organization
10 shall—

11 “(1) facilitate the exchange of information, best
12 practices, technical assistance, and support related
13 to the security of public, private, and critical infra-
14 structure information networks, including by—

15 “(A) ensuring that the information ex-
16 changed shall be stripped of all information
17 identifying the submitter and of any unneces-
18 sary personally identifiable information and
19 shall be available to members of the National
20 Information Sharing Organization, including
21 Federal, State, and local government agencies;
22 and

23 “(B) sharing timely and actionable threat
24 and vulnerability information originating
25 through intelligence collection with appro-

1 priately cleared members of the National Infor-
2 mation Sharing Organization;

3 “(2) create a common operating picture by
4 combining agreed upon network and cyber threat
5 warning information to be shared—

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

8 “(B) with designated members of the Na-
9 tional Information Sharing Organization, in-
10 cluding the Federal Government;

11 “(3) undertake collaborative research and devel-
12 opment projects to improve the level of cybersecurity
13 in critical infrastructure information systems while
14 maintaining impartiality, the independence of mem-
15 bers of the National Information Sharing Organiza-
16 tion, and vendor neutrality;

17 “(4) develop language to be incorporated into
18 the membership agreement regarding the transfer-
19 ability and use of intellectual property developed by
20 the National Information Sharing Organization and
21 its members under this subtitle; and

22 “(5) integrate with the Federal Government
23 through the National Cybersecurity and Communica-
24 tions Integration Center and other existing informa-
25 tion sharing and analysis centers, as appropriate.

1 **“SEC. 243. BOARD OF DIRECTORS.**

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

5 “(1) the executive and administrative operation
6 of the National Information Sharing Organization,
7 including matters relating to funding and promotion
8 of the National Information Sharing Organization;
9 and

10 “(2) ensuring and facilitating compliance by
11 members of the National Information Sharing Orga-
12 nization with the requirements of this subtitle.

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

15 “(1) One representative from the Department
16 of Homeland Security.

17 “(2) Four representatives from three different
18 Federal agencies with significant responsibility for
19 cybersecurity.

20 “(3) Ten representatives from the private sec-
21 tor, including at least one member representing a
22 small business interest and members representing
23 each of the following critical infrastructure sectors
24 and subsectors:

25 “(A) Banking and finance.

26 “(B) Communications.

1 “(C) Defense industrial base.

2 “(D) Energy, electricity subsector.

3 “(E) Energy, oil, and natural gas sub-
4 sector.

5 “(F) Health care and public health.

6 “(G) Information technology.

7 “(4) Two representatives from the privacy and
8 civil liberties community.

9 “(5) The Chair of the National Council of In-
10 formation Sharing and Analysis Centers.

11 “(c) INITIAL APPOINTMENT.—Not later than 30 days
12 after the date of the enactment of this subtitle, the Sec-
13 retary of Homeland Security, in consultation with the
14 heads of the sector specific agencies of the sectors and
15 subsectors referred to in subsection (b)(3), shall appoint
16 the members of the board described under subsection
17 (b)(3) from individuals identified by the sector coordi-
18 nating councils of sectors and subsectors referred to in
19 subsection (b)(3).

20 “(d) TERMS.—

21 “(1) REPRESENTATIVES OF CERTAIN FEDERAL
22 AGENCIES.—Each member of the board described in
23 subsection (b)(1) and (b)(2) shall be appointed for
24 a term that is not less than one year and not longer

1 than three years from the date of the member's ap-
2 pointment.

3 “(2) OTHER REPRESENTATIVES.—The original
4 private sector members of the board described sub-
5 section (b) shall serve an initial term of one year
6 from the date of appointment under subsection (c),
7 at which time the members of the National Informa-
8 tion Sharing Organization shall conduct elections in
9 accordance with the procedures established under
10 subsection (e).

11 “(e) RULES AND PROCEDURES.—Not later than 90
12 days after the date of the enactment of this Act, the board
13 shall establish rules and procedures for the election and
14 service of members of the board described in paragraphs
15 (3) and (4) of subsection (b).

16 “(f) LEADERSHIP.—The board shall elect from
17 among its members a chair and vice-chair of the board,
18 who shall serve under such terms and conditions as the
19 board may establish. The chair of the board may not be
20 a Federal employee.

21 “(g) SUB-BOARDS.—The board shall have the au-
22 thority to constitute such sub-boards, or other advisory
23 groups or panels, as may be necessary to assist the board
24 in carrying out its functions under this section. The board
25 shall establish an advisory group made up of the members

1 determined appropriate to participate in the common oper-
2 ation picture described in section 242(2) and to determine
3 information sets, sharing procedures, and operational pro-
4 tocols in creating the common operating picture.

5 **“SEC. 244. CHARTER.**

6 “The board shall develop a charter to govern the op-
7 erations and administration of the National Information
8 Sharing Organization. The charter shall cover each of the
9 following:

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

12 “(2) The governance of the National Informa-
13 tion Sharing Organization.

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

16 “(4) Criteria for membership of the National
17 Information Sharing Organization and for termi-
18 nation of such membership.

19 “(5) A funding model of the National Informa-
20 tion Sharing Organization, including costs, if any,
21 for membership.

22 “(6) Rules for sharing information with mem-
23 bers of the National Information Sharing Organiza-
24 tion, including the treatment and ownership of intel-
25 lectual property provided by or to the National In-

1 formation Sharing Organization, limitations on li-
2 ability, and consideration of any necessary measures
3 to mitigate anti-trust concerns.

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

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

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

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

17 “(11) Procedures for making anonymized cyber
18 incident information available to outside groups for
19 academic research and insurance actuarial purposes.

20 **“SEC. 245. MEMBERSHIP.**

21 “Not later than 90 days after the date of the enact-
22 ment of this subtitle, the board of directors of the National
23 Information Sharing Organization shall establish criteria
24 procedures for the voluntary membership by State and
25 local government departments, agencies, and entities, pri-

1 vate sector businesses and organizations, and academic in-
2 stitutions in the National Information Sharing Organiza-
3 tion.

4 **“SEC. 246. FUNDING.**

5 “Annual administrative and operational expenses for
6 the National Information Sharing Organization shall be
7 paid by the members of such Organization, as determined
8 by the board of directors of the Organization.

9 **“SEC. 247. CLASSIFIED INFORMATION.**

10 “Consistent with the protection of sensitive intel-
11 ligence sources and methods, the Secretary, in conjunction
12 with the Director of National Intelligence, shall facili-
13 tate—

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

21 “(2) the declassification and sharing of infor-
22 mation in the possession of a Federal agency related
23 to threats to information networks with members of
24 the National Information Sharing Organization.

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

2 “(a) IN GENERAL.—

3 “(1) CYBERSECURITY PROVIDERS.—Notwith-
4 standing any other provision of law, a cybersecurity
5 provider may, with the express consent of a pro-
6 tected entity for which such cybersecurity provider is
7 providing goods or services for cybersecurity pur-
8 poses, use cybersecurity systems to identify and ob-
9 tain cyber threat information to protect the rights
10 and property of such protected entity.

11 “(2) PROTECTED ENTITIES.—Notwithstanding
12 any other provision of law, a protected entity may,
13 for cybersecurity purposes—

14 “(A) share cyber threat information with
15 the National Information Sharing Organization
16 and its membership, including the Federal Gov-
17 ernment; or

18 “(B) authorize their cybersecurity provider
19 to share on their behalf with the National In-
20 formation Sharing Organization and its mem-
21 bership, including the Federal Government.

22 “(3) SELF-PROTECTED ENTITIES.—Notwith-
23 standing any other provision of law, a self-protected
24 entity may, for cybersecurity purposes—

25 “(A) use cybersecurity systems to identify
26 and obtain cyber threat information to protect

1 the rights and property of such self-protected
2 entity; and

3 “(B) share such cyber threat information
4 with the National Information Sharing Organi-
5 zation and its membership, including the Fed-
6 eral Government.

7 “(b) USES OF SHARED INFORMATION.—Notwith-
8 standing any other provision of law, information shared
9 with or provided to the National Information Sharing Or-
10 ganization or to a Federal agency or private entity
11 through the National Information Sharing Organization
12 by any member of the National Information Sharing Or-
13 ganization that is not a Federal agency in furtherance of
14 the mission and activities of the National Information
15 Sharing Organization as described in section 242—

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

19 “(2) shall not, without the written consent of
20 the person or entity submitting such information, be
21 used directly by any Federal agency, any other Fed-
22 eral, State, tribal, or local authority, or any third
23 party, in any civil action arising under Federal or
24 State law if such information is submitted to the
25 National Information Sharing Organization for the

1 purpose of facilitating the missions of such Organi-
2 zation, as articulated in the mission statement re-
3 quired under section 244;

4 “(3) shall not, without the written consent of
5 the person or entity submitting such information, be
6 used or disclosed by any officer or employee of the
7 United States for purposes other than the purposes
8 of this title, including any regulatory purpose, ex-
9 cept—

10 “(A) to further an investigation or the
11 prosecution of a cybersecurity related criminal
12 act; or

13 “(B) to disclose the information to the ap-
14 propriate congressional committee;

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

17 “(A) be made available pursuant to any
18 State or local law requiring disclosure of infor-
19 mation or records;

20 “(B) otherwise be disclosed or distributed
21 to any party by such State or local government
22 or government agency without the written con-
23 sent of the person or entity submitting such in-
24 formation; or

1 “(C) be used other than for the purpose of
2 protecting information systems, or in further-
3 ance of an investigation or the prosecution of a
4 criminal act;

5 “(5) does not constitute a waiver of any appli-
6 cable privilege or protection provided under law,
7 such as information that is proprietary, business
8 sensitive, relates specifically to the submitting per-
9 son or entity, or is otherwise not appropriately in
10 the public domain; and

11 “(6) shall not be the basis for any civil or crimi-
12 nal right of action in Federal or State court for a
13 failure to warn or disclose provided that the infor-
14 mation is shared with the Federal Government
15 through the National Information Sharing Organiza-
16 tion in accordance with the procedures established
17 under this section.

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

22 “(d) PROCEDURES.—

23 “(1) IN GENERAL.—Not later than 90 days
24 after the date of the enactment of this subtitle, the
25 board of directors of the National Information Shar-

1 ing Organization shall establish uniform procedures
2 for the receipt, care, and storage of information that
3 is voluntarily submitted to the Federal Government
4 through the National Information Sharing Organiza-
5 tion.

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

8 “(A) the acknowledgment of receipt by the
9 National Information Sharing Organization of
10 cyber threat information that is voluntarily sub-
11 mitted to the National Information Sharing Or-
12 ganization;

13 “(B) the maintenance of the identification
14 of such information;

15 “(C) the care and storage of such informa-
16 tion;

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

20 “(E) the protection of the privacy rights
21 and civil liberties of any individuals who are
22 subjects of such information; and

23 “(F) the protection and maintenance of
24 the confidentiality of such information so as to
25 permit the sharing of such information within

1 the Federal Government and with State, tribal,
2 and local governments, and the issuance of no-
3 tices and warnings related to the protection of
4 information networks, in such manner as to
5 protect from public disclosure the identity of
6 the submitting person or entity, or information
7 that is proprietary, business sensitive, relates
8 specifically to the submitting person or entity,
9 and is otherwise not appropriately in the public
10 domain.

11 “(e) INDEPENDENTLY OBTAINED INFORMATION.—
12 Nothing in this section shall be construed to limit or other-
13 wise affect the ability of a Federal agency, a State, tribal,
14 or local government or government agency, or any third
15 party—

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

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

21 “(f) DEFINITIONS.—In this section:

22 “(1) The term ‘cybersecurity provider’ means a
23 non-governmental entity that provides goods or serv-
24 ices intended to be used for cybersecurity purposes.

1 “(2) The term ‘cybersecurity purpose’ means
2 the purpose of ensuring the integrity, confidentiality,
3 or availability of, or safeguarding, a system or net-
4 work, including protecting a system or network
5 from—

6 “(A) efforts to degrade, disrupt or destroy
7 such system or network; or

8 “(B) theft or misappropriation of private
9 or government information, intellectual prop-
10 erty, or personally identifiable information.

11 “(3) The term ‘cybersecurity system’ means a
12 system designed or employed to ensure the integrity,
13 confidentiality, or availability of, or safeguarding, a
14 system or network, including protecting a system or
15 network from—

16 “(A) efforts to degrade, disrupt or destroy
17 such system or network; or

18 “(B) theft or misappropriation of private
19 or government information, intellectual prop-
20 erty, or personally identifiable information.

21 “(4) The term ‘cyber threat information’ means
22 information that is—

23 “(A) necessary to describe a method of de-
24 feating technical controls on a system or net-
25 work that corresponds to a cyber threat; and

1 “(B) omits all other information not nec-
2 essary to describe such threat.

3 “(5) The term ‘protected entity’ means an enti-
4 ty, other than an individual, that contracts with a
5 cybersecurity provider for goods or services to be
6 used for cybersecurity purposes.

7 “(6) The term ‘self-protected entity’ means an
8 entity, other than an individual, that provides goods
9 or services for cybersecurity purposes to itself.

10 **“SEC. 249. ANNUAL INDEPENDENT AUDITS.**

11 “The board of directors of the National Information
12 Sharing Organization shall commission, on an annual
13 basis, an audit by a qualified, independent auditing firm
14 approved by the Secretary, to review the compliance of the
15 National Information Sharing Organization and its mem-
16 bers with the information sharing rules set forth in section
17 248 and the information sharing rules established by the
18 board pursuant to the National Information Sharing Or-
19 ganization charter required under section 244. Such
20 audit—

21 “(1) shall identify instances in which informa-
22 tion may have been shared in a manner inconsistent
23 with procedures required under section 248 or with
24 the information sharing rules established by the
25 board pursuant to section 244, with the National In-

1 formation Sharing Organization, with members of
2 the National Information Sharing Organization, or
3 by the National Information Sharing Organization
4 with a National Information Sharing Organization
5 member or other entity or individual;

6 “(2) shall be provided to the Secretary and to
7 the Committee on Homeland Security of the House
8 of Representatives and to the Homeland Security
9 and Governmental Affairs Committee of the Senate;

10 “(3) shall be made public, with appropriate
11 redactions to protect the identity of National Infor-
12 mation Sharing Organization members; and

13 “(4) may include a classified annex.

14 **“SEC. 250. PENALTIES.**

15 “(a) IN GENERAL.—It shall be unlawful for any offi-
16 cer, employee, representative, or agent of the United
17 States or of any Federal agency, or any employee or offi-
18 cer of the National Information Sharing Organization, its
19 member entities, and any representatives or agents of the
20 National Information Sharing Organization or its member
21 entities to knowingly publish, divulge, disclose, or make
22 known in any manner or to any extent not authorized by
23 law, any cyber threat information protected from disclo-
24 sure by this title coming to such officer or employee in
25 the course of the employee’s employment or official duties

1 or by reason of any examination or investigation made by,
2 or return, report, or record made to or filed with, such
3 officer, employee, or agency.

4 “(b) PENALTY.—Any person who violates subsection
5 (a) shall be fined under title 18, United States Code, im-
6 prisoned for not more than one year, or both, and shall
7 be removed from office or employment.

8 **“SEC. 251. AUTHORITY TO ISSUE WARNINGS.**

9 “The Secretary may provide advisories, alerts, and
10 warnings to relevant companies, targeted sectors, other
11 government entities, or the general public regarding poten-
12 tial threats to information networks as appropriate. In
13 issuing such an advisory, alert, or warning, the Secretary
14 shall take appropriate actions to protect from disclosure—

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

18 “(2) information that is proprietary, business
19 sensitive, relates specifically to the submitting per-
20 son or entity, or is otherwise not appropriate for dis-
21 closure in the public domain.

22 **“SEC. 252. EXEMPTION FROM ANTITRUST PROHIBITIONS.**

23 “The exchange of information by and between private
24 sector members of the National Information Sharing Or-
25 ganization in furtherance of the mission and activities of

1 the National Information Sharing Organization shall not
2 be considered a violation of any provision of the antitrust
3 laws (as such term is defined in the first section of the
4 Clayton Act (15 U.S.C. 12)).

5 **“SEC. 253. LIMITATION.**

6 “For any fiscal year after fiscal year 2015, the
7 amount authorized to be appropriated for the National In-
8 formation Sharing Organization may not exceed the
9 amount provided by the largest private sector member of
10 the National Information Sharing Organization for that
11 fiscal year.”.

12 (2) CLERICAL AMENDMENT.—The table of con-
13 tents in section 2(b) of such Act, as amended by sec-
14 tion 2, is further amended by adding at the end of
15 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. Annual independent audits.

“Sec. 250. Penalties.

“Sec. 251. Authority to issue warnings.

“Sec. 252. Exemption from antitrust prohibitions.

“Sec. 253. Limitation.”.

16 (b) INITIAL EXPENSES.—There is authorized to be
17 appropriated \$10,000,000 for each of fiscal years 2013,
18 2014, and 2015 for initial expenses associated with the

1 establishment of the National Information Sharing Orga-
2 nization under subtitle E of title II of the Homeland Secu-
3 rity Act of 2002, as added by subsection (a). Such
4 amounts shall be derived from amounts appropriated for
5 the operations of the Management Office for the Direc-
6 torate of Science and Technology of the Department of
7 Homeland Security.

○