

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 3674  
OFFERED BY MR. DANIEL E. LUNGREN OF  
CALIFORNIA**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Promoting and En-  
3 hancing Cybersecurity and Information Sharing Effective-  
4 ness Act of 2011” or the “PRECISE Act of 2011”.

**5 SEC. 2. DEPARTMENT OF HOMELAND SECURITY  
6 CYBERSECURITY ACTIVITIES.**

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

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

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

16 “(1) develop and conduct risk assessments for  
17 Federal systems and, subject to the availability of

1 resources and upon request from critical infrastruc-  
2 ture owners and operators, critical infrastructure in-  
3 formation systems in consultation with the heads of  
4 other agencies or governmental and private entities  
5 that own and operate such systems, that may in-  
6 clude threat, vulnerability, and impact assessments  
7 and penetration testing, or other comprehensive as-  
8 sessments techniques;

9 “(2) foster the development, in conjunction with  
10 other governmental entities and the private sector,  
11 of essential information security technologies and ca-  
12 pabilities for protecting Federal systems and critical  
13 infrastructure information systems, including com-  
14 prehensive protective capabilities and other techno-  
15 logical solutions;

16 “(3) acquire, integrate, and facilitate the adop-  
17 tion of new cybersecurity technologies and practices  
18 in a technologically and vendor-neutral manner to  
19 keep pace with emerging terrorist and other  
20 cybersecurity threats and developments, including  
21 through research and development, technical service  
22 agreements, and making such technologies available  
23 to governmental and private entities that own or op-  
24 erate critical infrastructure information systems, as  
25 necessary to accomplish the purpose of this section;

1           “(4) establish and maintain a center to be  
2           known as the ‘National Cybersecurity and Commu-  
3           nications Integration Center’ to serve as a focal  
4           point with the Federal Government for  
5           cybersecurity, responsible for—

6                   “(A) the coordination of the protection of  
7           Federal systems and critical infrastructure in-  
8           formation systems;

9                   “(B) the coordination of national cyber in-  
10          cident response;

11                  “(C) facilitating information sharing, inter-  
12          actions, and collaborations among and between  
13          Federal agencies, State and local governments,  
14          the private sector, academia, and international  
15          partners;

16                  “(D) working with appropriate Federal  
17          agencies, State and local governments, the pri-  
18          vate sector, academia, and international part-  
19          ners to prevent and respond to terrorist and  
20          other cybersecurity threats and incidents involv-  
21          ing Federal systems and critical infrastructure  
22          information systems pursuant to the national  
23          cyber incident response plan and supporting  
24          plans developed in accordance with paragraph  
25          (8);

1           “(E) the dissemination of timely and ac-  
2           tionable terrorist and other cybersecurity  
3           threat, vulnerability, mitigation, and warning  
4           information, including alerts, advisories, indica-  
5           tors, signatures, and mitigation and response  
6           measures, to improve the security and protec-  
7           tion of Federal systems and critical infrastruc-  
8           ture information systems;

9           “(F) the integration of information from  
10          Federal Government and non-federal network  
11          operation centers and security operations cen-  
12          ters;

13          “(G) the compilation and analysis of infor-  
14          mation about risks and incidents regarding ter-  
15          rorism or other causes that threaten Federal  
16          systems and critical infrastructure information  
17          systems;

18          “(H) the provision of incident prediction,  
19          detection, analysis, mitigation, and response in-  
20          formation and remote or on-site technical as-  
21          sistance to heads of Federal agencies and, upon  
22          request, governmental and private entities that  
23          own or operate critical infrastructure; and

1           “(I) acting as the Federal Government  
2           representative with the organization or organi-  
3           zations designated under section 241;

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

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

11           “(A) the importance of cybersecurity and  
12          cyber ethics;

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  
17          cybersecurity workforce and educational paths  
18          to cybersecurity professions;

19          “(7) establish, in coordination with the Director  
20          of the National Institute of Standards and Tech-  
21          nology, the heads of other appropriate agencies, and  
22          appropriate elements of the private sector, guidelines  
23          for making critical infrastructure information sys-  
24          tems and industrial control systems more secure at  
25          a fundamental level, including through automation,

1 interoperability, and privacy-enhancing authentica-  
2 tion;

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

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

20 “(10) ensure that the technology and tools used  
21 to accomplish the requirements of this section are  
22 scientifically and operationally validated; and

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

1 “(b) COORDINATION.—

2 “(1) COORDINATION WITH OTHER ENTITIES.—

3 In carrying out the cybersecurity activities under  
4 this section, the Secretary shall coordinate, as ap-  
5 propriate, with—

6 “(A) the head of any relevant agency or  
7 entity;

8 “(B) representatives of State and local  
9 governments;

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

12 “(D) suppliers of technology for critical in-  
13 frastructure;

14 “(E) academia; and

15 “(F) international organizations and for-  
16 eign partners.

17 “(2) COORDINATION OF AGENCY ACTIVITIES.—

18 The Secretary shall coordinate the activities under-  
19 taken by agencies to protect Federal systems and  
20 critical infrastructure information systems and pre-  
21 pare the Nation to predict, anticipate, recognize, re-  
22 spond to, recover from, and mitigate against risk of  
23 acts of terrorism and other incidents involving such  
24 systems and infrastructure.

1           “(3) LEAD CYBERSECURITY OFFICIAL.—The  
2           Secretary shall designate a lead cybersecurity official  
3           to provide leadership to the cybersecurity activities  
4           of the Department and to ensure that the Depart-  
5           ment’s cybersecurity activities under this subtitle are  
6           coordinated with all other infrastructure protection  
7           and cyber-related programs and activities of the De-  
8           partment, including those of any intelligence or law  
9           enforcement components or entities within the De-  
10          partment.

11          “(4) REPORTS TO CONGRESS.—The lead  
12          cybersecurity official shall make annual reports to  
13          the appropriate committees of Congress on the co-  
14          ordination of cyber-related programs across the De-  
15          partment.

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

19               “(1) articulates the actions necessary to assure  
20               the readiness, reliability, continuity, integrity, and  
21               resilience of Federal systems and critical infrastruc-  
22               ture information systems;

23               “(2) includes explicit goals and objectives as  
24               well as specific timeframes for achievement of stated  
25               goals and objectives;

1           “(3) is informed by the need to maintain eco-  
2           nomic prosperity and facilitate market leadership for  
3           the United States information and communications  
4           industry; and

5           “(4) protects privacy rights and preserves civil  
6           liberties of United States persons.

7           “(d) ACCESS TO INFORMATION.—The Secretary shall  
8           ensure that the organization or organizations designated  
9           under section 241 have full and timely access to properly  
10          anonymized cyber incident information originating within  
11          the Federal civilian networks to populate the common op-  
12          erating picture described in section 242.

13          “(e) NO RIGHT OR BENEFIT.—The provision of as-  
14          sistance or information to governmental or private entities  
15          that own or operate critical infrastructure information sys-  
16          tems under this section shall be at the discretion of the  
17          Secretary and subject to the availability of resources. The  
18          provision of certain assistance or information to one gov-  
19          ernmental or private entity pursuant to this section shall  
20          not create a right or benefit, substantive or procedural,  
21          to similar assistance or information for any other govern-  
22          mental or private entity.

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

1 “(g) DEFINITIONS.—In this section:

2 “(1) The term ‘Federal systems’ means all in-  
3 formation systems owned, operated, leased, or other-  
4 wise controlled by an agency, or on behalf of an  
5 agency, except for national security systems or those  
6 information systems under the control of the De-  
7 partment of Defense.

8 “(2) The term ‘critical infrastructure informa-  
9 tion systems’ means any physical or virtual informa-  
10 tion system that controls, processes, transmits, re-  
11 ceives, or stores electronic information in any form,  
12 including data, voice, or video, that is—

13 “(A) vital to the functioning of critical in-  
14 frastructure as defined in section 5195c(e) of  
15 title 42, United States Code; or

16 “(B) owned or operated by or on behalf of  
17 a State or local government entity that is nec-  
18 essary to ensure essential government oper-  
19 ations continue.

20 “(h) AUTHORIZATION OF APPROPRIATION FOR THE  
21 NATIONAL CYBERSECURITY AND COMMUNICATIONS INTE-  
22 GRATION CENTER.—There is authorized to be appro-  
23 priated for the administration and management of the Na-  
24 tional Cybersecurity and Communications Integration  
25 Center established pursuant to subsection (a),

1 \$20,000,000 for each of fiscal years 2013, 2014, and  
2 2015.

3 **“SEC. 227. IDENTIFICATION OF SECTOR SPECIFIC**  
4 **CYBERSECURITY RISKS.**

5 “(a) IN GENERAL.—The Secretary shall, on a contin-  
6 uous and sector-by-sector basis, identify and evaluate  
7 cybersecurity risks to critical infrastructure for inclusion  
8 in annual risk assessments required under the National  
9 Infrastructure Protection Plan. In carrying out this sub-  
10 section, the Secretary shall coordinate, as appropriate,  
11 with the following:

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

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

16 “(3) The owners and operators of critical infra-  
17 structure, including as a priority, the relevant Crit-  
18 ical Infrastructure Partnership Advisory Council en-  
19 tities.

20 “(4) Any private sector entity determined ap-  
21 propriate by the Secretary.

22 “(b) EVALUATION OF RISKS.—The Secretary, in co-  
23 ordination with the individuals and entities referred to in  
24 subsection (a), shall evaluate the cybersecurity risks iden-

1 tified under subsection (a) by taking into account each of  
2 the following:

3           “(1) The actual or assessed threat, including a  
4           consideration of adversary capabilities and intent,  
5           preparedness, target attractiveness, and deterrence  
6           capabilities.

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

11          “(3) The threat to national security caused by  
12          the disruption, destruction or unauthorized use of  
13          critical infrastructure.

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

17          “(5) Other risk-based security factors that the  
18          Secretary, in consultation with the head of the sec-  
19          tor specific agency with responsibility for critical in-  
20          frastructure and the head of any Federal agency  
21          that is not a sector specific agency with responsibil-  
22          ities for regulating critical infrastructure, and in  
23          consultation with any private sector entity deter-  
24          mined appropriate by the Secretary to protect public

1 health and safety, critical infrastructure, or national  
2 and economic security.

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

8 “(d) COLLECTION OF RISK-BASED PERFORMANCE  
9 STANDARDS.—

10 “(1) REVIEW AND ESTABLISHMENT.—The Sec-  
11 retary, in coordination with the National Institute of  
12 Standards and Technology and the heads of other  
13 appropriate agencies, shall review existing inter-  
14 nationally recognized consensus-developed risk-based  
15 performance standards, including standards devel-  
16 oped by the National Institute of Standards and  
17 Technology, for inclusion in a common collection.  
18 Such collection shall include, for each such risk-  
19 based performance standard, an analysis, based on  
20 the typical implementation of each performance  
21 standard, of each of the following:

22 “(A) How well the performance standard  
23 addresses the identified risks.

1           “(B) How cost-effective the standard im-  
2           plementation of the performance standard can  
3           be.

4           “(2) USE OF COLLECTION.—The Secretary, in  
5           conjunction with the heads of other appropriate  
6           agencies, shall develop market-based incentives de-  
7           signed to encourage the use of the collection estab-  
8           lished under paragraph (1).

9           “(3) INCLUSION IN REGULATORY REGIMES.—  
10          The heads of sector specific agencies with responsi-  
11          bility for covered critical infrastructure and the head  
12          of any Federal agency that is not a sector specific  
13          agency with responsibilities for regulating covered  
14          critical infrastructure, in consultation with the Sec-  
15          retary and with any private sector entity determined  
16          appropriate by the Secretary, shall propose through  
17          notice and comment rulemaking to include the most  
18          effective and cost-efficient risk-based performance  
19          standards identified in the collection established  
20          under paragraph (1) in the regulatory regimes appli-  
21          cable to covered critical infrastructure.

22          “(e) MITIGATION OF RISKS.—If the Secretary deter-  
23          mines that no existing internationally-recognized risk-  
24          based performance standard mitigates a risk identified  
25          under subsection (a), the Secretary shall—

1           “(1) collaborate with owners and operators of  
2           critical infrastructure and suppliers of technology to  
3           develop mitigation strategies for the identified risk,  
4           including determining appropriate market-based in-  
5           centives for the implementation of the identified  
6           mitigation; and

7           “(2) engage with the National Institute of  
8           Standards and Technology and appropriate inter-  
9           national consensus bodies that develop and strength-  
10          en standards and practices to address the identified  
11          risk.

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

18                 “(1) a significant loss of life;

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

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

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

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

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

7           “(g) WRITTEN NOTIFICATION.—The Secretary shall  
8 provide written notification to the owners or operators of  
9 a facility or function that has been designated a covered  
10 critical infrastructure within 30 days of such designation.

11          “(h) REDRESS.—

12           “(1) IN GENERAL.—Subject to paragraphs (2)  
13 and (3), the Secretary shall develop a mechanism,  
14 consistent with subchapter II of chapter 5 of title 5,  
15 United States Code, for an owner or operator noti-  
16 fied under subsection (f) to appeal the identification  
17 of a facility or function as covered critical infrastruc-  
18 ture under this section.

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

24           “(3) COMPLIANCE.—The owner or operator of a  
25 facility or function identified as covered critical in-

1        frastructure shall comply with any requirement of  
2        this subtitle relating to covered critical infrastruc-  
3        ture until such time as the facility or function is no  
4        longer identified as covered critical infrastructure,  
5        based on—

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

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

9                “(C) a final judgment entered in a civil ac-  
10        tion seeking judicial review brought in accord-  
11        ance with paragraph (2).

12    **“SEC. 228. INFORMATION SHARING.**

13        “(a) CYBERSECURITY INFORMATION.—The Secretary  
14        shall be responsible for making all cyber threat informa-  
15        tion, provided pursuant to section 202 of this title, avail-  
16        able to appropriate owners and operators of critical infra-  
17        structure on a timely basis consistent with the responsibil-  
18        ities of the Secretary to provide information related to  
19        threats to critical infrastructures to the organization des-  
20        ignated under section 241.

21        “(b) INFORMATION SHARING.—The Secretary shall,  
22        in a timely manner and to the maximum extent possible,  
23        consistent with rules for the handling of classified and sen-  
24        sitive but unclassified information, share relevant informa-  
25        tion regarding cybersecurity threats and vulnerabilities,

1 and any proposed actions to mitigate them, with all Fed-  
2 eral agencies, appropriate State or local government rep-  
3 resentatives, and appropriate critical infrastructure infor-  
4 mation systems owners and operators, including by expe-  
5 diting necessary security clearances for designated points  
6 of contact for critical infrastructure information systems.

7 “(c) PROTECTION OF INFORMATION.—The Secretary  
8 shall designate, as appropriate, information received from  
9 Federal agencies and from critical infrastructure informa-  
10 tion systems owners and operators and information pro-  
11 vided to Federal agencies or critical infrastructure infor-  
12 mation systems owners and operators pursuant to this sec-  
13 tion as sensitive security information and shall require and  
14 enforce sensitive security information requirements for  
15 handling, storage, and dissemination of any such informa-  
16 tion, including proper protections for personally identifi-  
17 able information and stripping data of unnecessary identi-  
18 fying information.

19 **“SEC. 229. CYBERSECURITY RESEARCH AND DEVELOP-**  
20 **MENT.**

21 “(a) IN GENERAL.—The Under Secretary for Science  
22 and Technology shall support research, development, test-  
23 ing, evaluation, and transition of cybersecurity technology  
24 in coordination with a national cybersecurity research and  
25 development plan. Such support shall include funda-

1 mental, long-term research to improve the ability of the  
2 United States to prevent, protect against, detect, respond  
3 to, and recover from acts of terrorism and cyber attacks,  
4 with an emphasis on research and development relevant  
5 to attacks that would cause a debilitating impact on na-  
6 tional security, national economic security, or national  
7 public health and safety.

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

11 “(1) advance the development and accelerate  
12 the deployment of more secure versions of funda-  
13 mental Internet protocols and architectures, includ-  
14 ing for the domain name system and routing proto-  
15 cols;

16 “(2) improve, create, and advance the research  
17 and development of techniques and technologies for  
18 proactive detection and identification of threats, at-  
19 tacks, and acts of terrorism before they occur;

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

23 “(4) improve and create mitigation and recov-  
24 ery methodologies, including techniques and policies

1 for real-time containment of attacks and develop-  
2 ment of resilient networks and systems;

3 “(5) develop and support infrastructure and  
4 tools to support cybersecurity research and develop-  
5 ment efforts, including modeling, test beds, and data  
6 sets for assessment of new cybersecurity tech-  
7 nologies;

8 “(6) assist in the development and support of  
9 technologies to reduce vulnerabilities in process con-  
10 trol systems;

11 “(7) develop and support cyber forensics and  
12 attack attribution;

13 “(8) test, evaluate, and facilitate the transfer of  
14 technologies associated with the engineering of less  
15 vulnerable software and securing the information  
16 technology software development lifecycle; and

17 “(9) ensure new cybersecurity technologies are  
18 scientifically and operationally validated.

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

21 “(1) the Under Secretary for National Protec-  
22 tion and Programs Directorate; and

23 “(2) the heads of other relevant Federal depart-  
24 ments and agencies, including the National Science  
25 Foundation, the Defense Advanced Research

1 Projects Agency, the Information Assurance Direc-  
2 torate of the National Security Agency, the National  
3 Institute of Standards and Technology, the Depart-  
4 ment of Commerce, academic institutions, the Net-  
5 working and Information Technology Research and  
6 Development Program, and other appropriate work-  
7 ing groups established by the President to identify  
8 unmet needs and cooperatively support activities, as  
9 appropriate.

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

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

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

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

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

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

23          “(d) ANNUAL REPORT.—Not later than one year  
24          after the date of the enactment of this section, and annu-  
25          ally thereafter, the Secretary shall submit to the Com-

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

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

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

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

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

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

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

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

22           “(3) long-term and short-term strategic goals to  
23           address critical skills deficiencies, including an anal-  
24           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. 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.”.

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 igned 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 the organization or organizations to  
3 function as the National Information Sharing Organiza-  
4 tion by taking into consideration the following criteria and  
5 other criteria found appropriate by the board:

6           “(1) Whether the organization or organizations  
7 have received recognition from the Secretary of  
8 Homeland Security for its cyber capabilities.

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

13           “(3) Whether the organization or organizations  
14 have demonstrated the capability to deploy  
15 cybersecurity services for the detection, prevention,  
16 and mitigation of cyber-related issues.

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

21           “(5) Whether the organization or organizations  
22 have a proven relationship with the private sector  
23 critical infrastructure sectors.

24           “(6) Whether the organization or organizations  
25 have experience implementing privacy protections to

1       safeguard, sensitive information, including person-  
2       ally identifiable information, in transit and at rest.

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

4       “The National Information Sharing Organization  
5 shall—

6               “(1) facilitate the exchange of information, best  
7       practices, technical assistance, and support related  
8       to the security of public, private, and critical infra-  
9       structure information networks and to improve the  
10      effectiveness of the National Cyber Incident Re-  
11      sponse Plan, including by—

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

20               “(B) sharing timely and actionable threat  
21      and vulnerability information originating  
22      through intelligence collection with appropriate  
23      members of the National Information Sharing  
24      Organization;

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

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

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

9           “(3) facilitate collaborative research and devel-  
10 opment projects funded by members of the National  
11 Information Sharing Organization to improve the  
12 level of cybersecurity in critical infrastructure infor-  
13 mation systems while maintaining impartiality, the  
14 independence of the members of the National Infor-  
15 mation Sharing Organization, and vendor neutrality;

16           “(4) develop language to be incorporated into  
17 the membership agreement regarding the transfer-  
18 ability and use of intellectual property developed by  
19 the National Information Sharing Organization and  
20 its members under this subtitle ensuring that all  
21 members comply with all applicable intellectual prop-  
22 erty laws; and

23           “(5) integrate with the Federal Government  
24 through the National Cybersecurity and Communica-

1        tions Integration Center and other existing informa-  
2        tion sharing and analysis centers, as appropriate.

3        **“SEC. 243. BOARD OF DIRECTORS.**

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

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

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

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

17              “(1) One representative from the Department  
18              of Homeland Security.

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

22              “(3) Ten representatives from the private sec-  
23              tor, including at least one member representing a  
24              small business interest and members representing

1 each of the following critical infrastructure sectors  
2 and subsectors:

3 “(A) Banking and finance.

4 “(B) Communications.

5 “(C) Defense industrial base.

6 “(D) Energy, electricity subsector.

7 “(E) Energy, oil, and natural gas sub-  
8 sector.

9 “(F) Health care and public health.

10 “(G) Information technology.

11 “(H) Water.

12 “(4) Two representatives from the privacy and  
13 civil liberties community.

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

16 “(c) INITIAL APPOINTMENT.—Not later than 30 days  
17 after the date of the enactment of this subtitle, the Sec-  
18 retary of Homeland Security, in consultation with the  
19 heads of the sector specific agencies of the critical infra-  
20 structure sectors enumerated in the National Infrastruc-  
21 ture Protection Plan, shall appoint the members of the  
22 board described under subsection (b)(3) from individuals  
23 identified by the sector coordinating councils of the critical  
24 infrastructure sectors enumerated in the National Infra-  
25 structure Protection Plan.

1 “(d) TERMS.—

2 “(1) REPRESENTATIVES OF CERTAIN FEDERAL  
3 AGENCIES.—Each member of the board described in  
4 subsection (b)(1) and (b)(2) shall be appointed for  
5 a term that is not less than one year and not longer  
6 than three years from the date of the member’s ap-  
7 pointment.

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

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

21 “(f) LEADERSHIP.—The board shall elect from  
22 among its members a chair and vice-chair of the board,  
23 who shall serve under such terms and conditions as the  
24 board may establish. The chair of the board may not be  
25 a Federal employee.

1           “(g) SUB-BOARDS.—The board shall have the au-  
2 thority to constitute such sub-boards, or other advisory  
3 groups or panels, as may be necessary to assist the board  
4 in carrying out its functions under this section. The board  
5 shall establish an advisory group made up of the members  
6 determined appropriate to participate in the common oper-  
7 ation picture described in section 242(2) and to determine  
8 information sets, sharing procedures, and operational pro-  
9 tocols in creating the common operating picture.

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.

24           “(5) A funding model of the National Informa-  
25 tion Sharing Organization, including a fee scale that

1 includes a sliding scale for membership fees for  
2 small businesses and promotes broad participation  
3 by large, medium, and small business owners and  
4 operators of networks or systems in the private sec-  
5 tor, entities operating critical infrastructure, edu-  
6 cational institutions, State, tribal, and local govern-  
7 ments, and the Federal Government.

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

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

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

21 “(9) Protections of privacy and civil liberties to  
22 be used by the National Information Sharing Orga-  
23 nization and its members, including appropriate  
24 measures—

25 “(A) for public transparency and oversight;

1           “(B) to ensure that only cyber threat in-  
2           formation is shared with and by the National  
3           Information Sharing Organization; and

4           “(C) to omit personally identifiable infor-  
5           mation not necessary to describe a cyber threat  
6           from information shared with and by the Na-  
7           tional Information Sharing Organization.

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

11          “(11) Procedures for coordinating cooperative  
12          research and development projects funded by mem-  
13          bers of the National Information Sharing Organiza-  
14          tion with the Science and Technology Directorate  
15          and the Networking and Information Technology  
16          Research and Development Program.

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

20          “(13) Procedures for the incorporation of inter-  
21          national entities and allied government agencies into  
22          the membership of the National Information Sharing  
23          Organization.

1           “(14) Any other provision determined necessary  
2           by the Board to advance the purpose of the National  
3           Information Sharing Organization.

4   **“SEC. 245. MEMBERSHIP.**

5           “Not later than 90 days after the date of the enact-  
6           ment of this subtitle, the board of directors of the National  
7           Information Sharing Organization shall establish criteria  
8           procedures for the voluntary membership by State and  
9           local government departments, agencies, and entities, pri-  
10          vate sector businesses and organizations, and academic in-  
11          stitutions in the National Information Sharing Organiza-  
12          tion.

13   **“SEC. 246. FUNDING.**

14          “Annual administrative and operational expenses for  
15          the National Information Sharing Organization shall be  
16          paid by the members of such Organization, as determined  
17          by the board of directors of the Organization.

18   **“SEC. 247. CLASSIFIED INFORMATION.**

19          “Consistent with the protection of sensitive intel-  
20          ligence sources and methods, the Secretary, in conjunction  
21          with the heads of appropriate Federal agencies, shall fa-  
22          cilitate, through the National Cybersecurity and Commu-  
23          nications Integration Center—

24                  “(1) the sharing of classified cybersecurity  
25          threat information in the possession of a Federal

1 agency related to threats to information networks  
2 with cleared members of the National Information  
3 Sharing Organization, including representatives of  
4 the private sector and of public and private sector  
5 entities operating critical infrastructure; and

6 “(2) the declassification and sharing of  
7 cybersecurity threat information in the possession of  
8 a Federal agency related to threats to information  
9 networks with members of the National Information  
10 Sharing Organization.

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

12 “(a) IN GENERAL.—

13 “(1) CYBERSECURITY PROVIDERS.—Notwith-  
14 standing any other provision of law, a cybersecurity  
15 provider may, with the express consent of a pro-  
16 tected entity for which such cybersecurity provider is  
17 providing goods or services for cybersecurity pur-  
18 poses, use cybersecurity systems to identify and ob-  
19 tain cyber threat information to protect the rights  
20 and property of such protected entity.

21 “(2) PROTECTED ENTITIES.—Notwithstanding  
22 any other provision of law, a protected entity may,  
23 for cybersecurity purposes—

24 “(A) share cyber threat information with  
25 the National Information Sharing Organization

1 and its membership, including the Federal Gov-  
2 ernment; or

3 “(B) authorize their cybersecurity provider  
4 to share cyber threat information on their be-  
5 half with the National Information Sharing Or-  
6 ganization and its membership, including the  
7 Federal Government.

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

11 “(A) use cybersecurity systems to identify  
12 and obtain cyber threat information to protect  
13 the rights and property of such self-protected  
14 entity; and

15 “(B) share such cyber threat information  
16 with the National Information Sharing Organi-  
17 zation and its membership, including the Fed-  
18 eral Government.

19 “(b) USES OF SHARED INFORMATION.—Notwith-  
20 standing any other provision of law, information shared  
21 with or provided to the National Information Sharing Or-  
22 ganization or to a Federal agency or private entity  
23 through the National Information Sharing Organization  
24 by any member of the National Information Sharing Or-  
25 ganization that is not a Federal agency in furtherance of

1 the mission and activities of the National Information  
2 Sharing Organization as described in section 242—

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

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

16 “(3) shall not be used or disclosed by any offi-  
17 cer or employee of the United States for purposes  
18 other than a cybersecurity purpose, including any  
19 regulatory purpose, except—

20 “(A) to further an investigation or the  
21 prosecution of a cybersecurity related criminal  
22 act; or

23 “(B) to disclose the information to the ap-  
24 propriate congressional committee;

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

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

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

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

15           “(5) shall not, if subsequently provided to a pri-  
16 vate entity, be used for any purpose other than a  
17 cybersecurity purpose;

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

24           “(7) shall not be the basis for any tort action  
25 or criminal right of action in Federal or State court

1 for a failure to warn or disclose provided that the in-  
2 formation is shared with the Federal Government  
3 through the National Information Sharing Organiza-  
4 tion in accordance with the procedures established  
5 under this section.

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

10 “(d) PROCEDURES.—

11 “(1) IN GENERAL.—Not later than 90 days  
12 after the date of the enactment of this subtitle, the  
13 board of directors of the National Information Shar-  
14 ing Organization shall establish uniform procedures  
15 for the receipt, care, and storage of information that  
16 is voluntarily submitted to the Federal Government  
17 through the National Information Sharing Organiza-  
18 tion.

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

21 “(A) the acknowledgment of receipt by the  
22 National Information Sharing Organization of  
23 cyber threat information that is voluntarily sub-  
24 mitted to the National Information Sharing Or-  
25 ganization;

1           “(B) the maintenance of the identification  
2 of such information;

3           “(C) the care and storage of such informa-  
4 tion;

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

8           “(E) the protection of the privacy rights  
9 and civil liberties of any individuals who are  
10 subjects of such information; and

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

24           “(e) INDEPENDENTLY OBTAINED INFORMATION.—

25 Nothing in this section shall be construed to limit or other-

1 wise affect the ability of a Federal agency, a State, tribal,  
2 or local government or government agency, or any third  
3 party—

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

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

9 “(f) DEFINITIONS.—In this section:

10 “(1) The term ‘cyber attack’ means the inten-  
11 tional use of a wire or electronic communication to  
12 access or attempt to access without authorization or  
13 in excess of authorization a protected computer in a  
14 manner that subverts a technical control and in so  
15 doing—

16 “(A) causes or attempts to cause the modi-  
17 fication, destruction, or disclosure of informa-  
18 tion;

19 “(B) causes or attempts to cause damage  
20 and loss; or

21 “(C) renders or attempts to render infor-  
22 mation in a protected computer, or the com-  
23 puter itself, unavailable.

1           “(2) The term ‘cybersecurity related criminal  
2 act’ means conduct that is already a crime under  
3 Federal or State law that involves—

4           “(A) efforts to degrade, disrupt or destroy  
5 a cybersecurity system or network; or

6           “(B) theft or misappropriation of private  
7 or government information, intellectual property  
8 or personally identifiable information from an  
9 information system or network.

10          “(3) The term ‘cybersecurity provider’ means a  
11 non-governmental entity that provides goods or serv-  
12 ices intended to be used for cybersecurity purposes.

13          “(4) The term ‘cybersecurity purpose’ means  
14 the purpose of ensuring the integrity, confidentiality,  
15 or availability of, or safeguarding, a system or net-  
16 work, including protecting a system or network  
17 from—

18          “(A) efforts to degrade, disrupt or destroy  
19 such system or network; or

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

23          “(5) The term ‘cybersecurity system’ means a  
24 system designed or employed to ensure the integrity,  
25 confidentiality, or availability of, or safeguarding, a

1 system or network, including protecting a system or  
2 network from—

3 “(A) efforts to degrade, disrupt or destroy  
4 such system or network; or

5 “(B) theft or misappropriation of private  
6 or government information, intellectual prop-  
7 erty, or personally identifiable information.

8 “(6) The term ‘cyber threat information’ means  
9 the information—

10 “(A) that is necessary to identify or de-  
11 scribe—

12 “(i) a method of defeating a technical  
13 or operational control that corresponds to  
14 a cyber attack;

15 “(ii) a method of causing a person  
16 with authorized access to an information  
17 system or to information that is stored on,  
18 processed by, or transiting an information  
19 system to unwittingly enable the defeat of  
20 a technical control;

21 “(iii) information exfiltrated in a  
22 cyber attack when such information nec-  
23 essary to identify or describe the attack;

24 “(iv) anomalous patterns of commu-  
25 nications that appear to be transmitted in

1 connection with a cyber attack, but does  
2 not include other communications content,  
3 or dialing, routing, addressing and sig-  
4 naling information not necessary to de-  
5 scribe such attack;

6 “(v) anomalous patterns of commu-  
7 nications that appear to be transmitted for  
8 the purpose of gathering technical informa-  
9 tion to be used in a cyber attack; or

10 “(vi) a method for remote identifica-  
11 tion of, access to, or use of an information  
12 system or information that is stored on,  
13 processed by, or transiting an information  
14 system associated with a known or sus-  
15 pected cyber attack; and

16 “(B) from which reasonable efforts have  
17 been made to remove information that can be  
18 used to identify specific persons unrelated to a  
19 cyber attack.

20 “(7) The term ‘technical control’ means a hard-  
21 ware or software restriction on access or use of a  
22 protected computer or information in a protected  
23 computer that is intended to ensure the confiden-  
24 tiality, integrity, or availability of that computer or  
25 information.

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

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

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

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

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

1 by the National Information Sharing Organization  
2 with a National Information Sharing Organization  
3 member or other entity or individual;

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

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

11 “(4) may include a classified annex.

12 **“SEC. 250. PENALTIES.**

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

1 or return, report, or record made to or filed with, such  
2 officer, employee, or agency.

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

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

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

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

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

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

22 “The exchange of information by and between private  
23 sector members of the National Information Sharing Or-  
24 ganization in furtherance of the mission and activities of  
25 the National Information Sharing Organization shall not

1 be considered a violation of any provision of the antitrust  
2 laws (as such term is defined in the first section of the  
3 Clayton Act (15 U.S.C. 12)).

4 **“SEC. 253. LIMITATION.**

5 “(a) NO APPROPRIATIONS.—For any fiscal year after  
6 fiscal year 2015, no Federal appropriations shall be au-  
7 thorized for the National Information Sharing Organiza-  
8 tion.

9 “(b) MEMBERSHIP FEES FOR FEDERAL AGEN-  
10 CIES.—Membership fees for the National Information  
11 Sharing Organization shall not be collected from the Fed-  
12 eral Government for any fiscal year prior to fiscal year  
13 2015 and the Federal Government shall not be assessed  
14 a fee in excess of the fee collected from the largest private  
15 sector member of the National Information Sharing Orga-  
16 nization.’”.

17 (2) CLERICAL AMENDMENT.—The table of con-  
18 tents in section 2(b) of such Act, as amended by sec-  
19 tion 2, is further amended by adding at the end of  
20 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.”.

1           (b) INITIAL EXPENSES.—There is authorized to be  
2 appropriated \$10,000,000 for each of fiscal years 2013,  
3 2014, and 2015 for initial expenses associated with the  
4 establishment of the National Information Sharing Orga-  
5 nization under subtitle E of title II of the Homeland Secu-  
6 rity Act of 2002, as added by subsection (a). Such  
7 amounts shall be derived from amounts appropriated for  
8 the operations of the Management Office for the Direc-  
9 torate of Science and Technology of the Department of  
10 Homeland Security.

11 **SEC. 4. REPORT ON SUPPORT FOR REGIONAL**  
12 **CYBERSECURITY COOPERATIVES.**

13           Not later than 180 days after the date of the enact-  
14 ment of this Act, the Secretary of Homeland Security shall  
15 submit to the Committee on Homeland Security of the  
16 House of Representatives and the Committee on Home-  
17 land Security and Governmental Affairs of the Senate a  
18 report on the Secretary’s plan to provide support to re-  
19 gional, State, and local grassroots cyber cooperatives de-  
20 signed to decrease cyber disruptions to critical infrastruc-  
21 ture, increase cyber workforce training efforts, increase  
22 community awareness of cybersecurity, organize commu-  
23 nity cyber-emergency preparedness efforts, build resiliency  
24 of regional, State, and local critical services, and coordi-

1 nate academic technical and policy research effort. The re-  
2 port shall include each of the following:

3 (1) A plan for introducing a grant process for  
4 pilot regional, State, and local cyber cooperatives  
5 that would be implemented within 90 days of the  
6 submission of the report to Congress.

7 (2) Recommendations for integrating regional,  
8 State, and local grassroots cyber cooperatives in re-  
9 gional, State, and Federal cyber disruption plans.

10 (3) A plan for increasing cyber threat informa-  
11 tion sharing between regional, State, and local cyber  
12 cooperatives, the Federal Emergency Management  
13 Agency, the Department of Homeland Security, and  
14 the National Information Sharing Organization.

15 (4) A plan to promote with the National Infor-  
16 mation Sharing Organization a ground up, commu-  
17 nity-based network of cyber cooperatives.

18 (5) A plan for establishing a Federal online  
19 portal for existing groups to coordinate online train-  
20 ing, best practices, and other cybersecurity integra-  
21 tion efforts.

22 (6) A plan for utilizing Federal cyber assets in  
23 support of disaster response efforts, as well as sup-  
24 port to regional, State, and local cyber cooperatives.

1 **SEC. 5. PILOT PROGRAM ON CYBERSECURITY TRAINING**  
2 **FOR FUSION CENTERS.**

3 (a) PLAN.—The Secretary of Homeland Security  
4 shall develop a plan to implement a one-year voluntary  
5 pilot program to test and assess the feasibility, costs, and  
6 benefits of providing cybersecurity training to State and  
7 local law enforcement personnel through the national net-  
8 work of fusion centers.

9 (b) PILOT PROGRAM.—

10 (1) IN GENERAL.—Not later than one year  
11 after the date of the enactment of the Act, the Sec-  
12 retary shall implement a one-year voluntary pilot  
13 program to train State and local law enforcement  
14 personnel in the national network of fusion centers  
15 in cyber security standards, procedures, and best  
16 practices.

17 (2) CURRICULUM AND PERSONNEL.—In cre-  
18 ating the curriculum for the training program and  
19 conducting the program, the Secretary may assign  
20 personnel from the Department of Homeland Secu-  
21 rity, including personnel from the Office of  
22 Cybersecurity and Communications.

23 **SEC. 6. ASSESSMENT OF SECTOR BY SECTOR**  
24 **CYBERSECURITY PREPAREDNESS.**

25 (a) ASSESSMENT REQUIRED.—The Secretary of  
26 Homeland Security, in conjunction with the owners and

1 operators of critical infrastructure through the Critical In-  
2 frastructure Partnership Advisory Council, and in con-  
3 sultation with the sector specific agencies and agencies  
4 with regulatory authority over critical infrastructure, and  
5 other appropriate organizations shall conduct an assess-  
6 ment of the cybersecurity preparedness of each sector of  
7 the critical infrastructure as described in the National In-  
8 frastructure Protection Plan. Not later than 180 days  
9 after the date of the enactment of this Act, the Secretary  
10 shall submit to the appropriate congressional committees  
11 the results and recommendations of that assessment in an  
12 unclassified report, with a classified annex if appropriate.

13 (b) CONTENTS OF REPORT.— The report required by  
14 subsection (a) shall include an assessment of the current  
15 state of the cybersecurity preparedness of each sector, in-  
16 cluding an evaluation of—

17 (1) the current state of cybersecurity situational  
18 awareness for each sector, an articulation of what an  
19 adequate level of cybersecurity situational awareness  
20 should be for the sector, and recommendations for  
21 how and over what time frame the gap should be  
22 closed between current and desired end-state;

23 (2) the current state of cybersecurity analytic  
24 capability for each sector, an articulation of what an  
25 adequate level of cybersecurity analytic capability

1 should be for the sector, and recommendations for  
2 how and over what time frame the gap should be  
3 closed between current and desired end-state;

4 (3) the current state of cybersecurity response  
5 capability for each sector, an articulation of what an  
6 adequate level of cybersecurity response capability  
7 should be for the sector, and recommendations for  
8 how and over what time frame the gap should be  
9 closed between current and desired end-state; and

10 (4) the current state of cybersecurity recovery  
11 planning and capability for each sector, an articula-  
12 tion of what an adequate level of recovery planning  
13 and capability should be for the sector, and rec-  
14 ommendations for how and over what time frame the  
15 gap should be closed between current and desired  
16 end-state.

17 (c) CYBERSECURITY RISK.—To the extent necessary  
18 to inform the quality and specificity of the evaluation and  
19 recommendations regarding cybersecurity preparedness  
20 for each sector, consideration should be given to the  
21 cybersecurity identified under section 227 of the Home-  
22 land Security Act of 2002, as added by this Act.

