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:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011'' or the ''PRECISE Act of 2011''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY ACTIVITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 is amended by adding at the end the following new sections:

''SEC. 226. NATIONAL CYBERSECURITY AUTHORITY.

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

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

resources and upon request from critical infrastructure owners and operators, critical infrastructure information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing, or other comprehensive assessments techniques;

''(2) foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting Federal systems and critical infrastructure information systems, including comprehensive protective capabilities and other technological solutions;

''(3) acquire, integrate, and facilitate the adoption of new cybersecurity technologies and practices in a technologically and vendor-neutral manner to keep pace with emerging terrorist and other cybersecurity threats and developments, including through research and development, technical service agreements, and making such technologies available to governmental and private entities that own or operate critical infrastructure information systems, as necessary to accomplish the purpose of this section;

''(4) establish and maintain a center to be known as the 'National Cybersecurity and Communications Integration Center' to serve as a focal point with the Federal Government for cybersecurity, responsible for—

''(A) the coordination of the protection of Federal systems and critical infrastructure information systems;

''(B) the coordination of national cyber incident response;

''(C) facilitating information sharing, interactions, and collaborations among and between Federal agencies, State and local governments, the private sector, academia, and international partners;

''(D) working with appropriate Federal agencies, State and local governments, the private sector, academia, and international partners to prevent and respond to terrorist and other cybersecurity threats and incidents involving Federal systems and critical infrastructure information systems pursuant to the national cyber incident response plan and supporting plans developed in accordance with paragraph (8);

''(E) the dissemination of timely and actionable terrorist and other cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of Federal systems and critical infrastructure information systems;

''(F) the integration of information from Federal Government and non-federal network operation centers and security operations centers;

''(G) the compilation and analysis of information about risks and incidents regarding terrorism or other causes that threaten Federal systems and critical infrastructure information systems;

''(H) the provision of incident prediction, detection, analysis, mitigation, and response information and remote or on-site technical assistance to heads of Federal agencies and, upon request, governmental and private entities that own or operate critical infrastructure; and

''(I) acting as the Federal Government representative with the organization or organizations designated under section 241;

''(5) assist in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and the resiliency of Federal systems and critical infrastructure information systems;

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

''(A) the importance of cybersecurity and cyber ethics;

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

''(C) training opportunities to support the development of an effective national cybersecurity workforce and educational paths to cybersecurity professions;

''(7) establish, in coordination with the Director of the National Institute of Standards and Technology, the heads of other appropriate agencies, and appropriate elements of the private sector, guidelines for making critical infrastructure information systems and industrial control systems more secure at a fundamental level, including through automation,

interoperability, and privacy-enhancing authentication;

''(8) develop a national cybersecurity incident response plan and supporting cyber incident response and restoration plans, in consultation with the heads of other relevant Federal agencies, owners and operators of critical infrastructure, sector coordinating councils, State and local governments, and relevant non-governmental organizations and based on applicable law that describe the specific roles and responsibilities of governmental and private entities during cyber incidents to ensure essential government operations continue;

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

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

''(11) take such other lawful action as may be necessary and appropriate to accomplish the requirements of this section.

''(b) COORDINATION.—

''(1) COORDINATION WITH OTHER ENTITIES.—In carrying out the cybersecurity activities under this section, the Secretary shall coordinate, as appropriate, with—

''(A) the head of any relevant agency or entity;

''(B) representatives of State and local governments;

''(C) the private sector, including owners and operators of critical infrastructure;

''(D) suppliers of technology for critical infrastructure;

''(E) academia; and

''(F) international organizations and foreign partners.

''(2) COORDINATION OF AGENCY ACTIVITIES.—The Secretary shall coordinate the activities undertaken by agencies to protect Federal systems and critical infrastructure information systems and prepare the Nation to predict, anticipate, recognize, respond to, recover from, and mitigate against risk of acts of terrorism and other incidents involving such systems and infrastructure.

''(3) LEAD CYBERSECURITY OFFICIAL.—The Secretary shall designate a lead cybersecurity official to provide leadership to the cybersecurity activities of the Department and to ensure that the Department's cybersecurity activities under this subtitle are coordinated with all other infrastructure protection and cyber-related programs and activities of the Department, including those of any intelligence or law enforcement components or entities within the Department.

''(4) REPORTS TO CONGRESS.—The lead cybersecurity official shall make annual reports to the appropriate committees of Congress on the coordination of cyber-related programs across the Department.

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

''(1) articulates the actions necessary to assure the readiness, reliability, continuity, integrity, and resilience of Federal systems and critical infrastructure information systems;

''(2) includes explicit goals and objectives as well as specific timeframes for achievement of stated goals and objectives;

''(3) is informed by the need to maintain economic prosperity and facilitate market leadership for the United States information and communications industry; and

''(4) protects privacy rights and preserves civil liberties of United States persons.

''(d) ACCESS TO INFORMATION.—The Secretary shall ensure that the organization or organizations designated under section 241 have full and timely access to properly anonymized cyber incident information originating within the Federal civilian networks to populate the common operating picture described in section 242.

''(e) NO RIGHT OR BENEFIT.—The provision of assistance or information to governmental or private entities that own or operate critical infrastructure information systems under this section shall be at the discretion of the Secretary and subject to the availability of resources. The provision of certain assistance or information to one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

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

''(g) DEFINITIONS.—In this section:

''(1) The term 'Federal systems' means all information systems owned, operated, leased, or otherwise controlled by an agency, or on behalf of an agency, except for national security systems or those information systems under the control of the Department of Defense.

''(2) The term 'critical infrastructure information systems' means any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form, including data, voice, or video, that is—

''(A) vital to the functioning of critical infrastructure as defined in section 5195c(e) of title 42, United States Code; or

''(B) owned or operated by or on behalf of a State or local government entity that is necessary to ensure essential government operations continue.

''(h) AUTHORIZATION OF APPROPRIATION FOR THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.—There is authorized to be appropriated for the administration and management of the National Cybersecurity and Communications Integration Center established pursuant to subsection (a),

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

"SEC. 227. IDENTIFICATION OF SECTOR SPECIFIC CYBERSECURITY RISKS.

"(a) IN GENERAL.—The Secretary shall, on a continuous and sector-by-sector basis, identify and evaluate cybersecurity risks to critical infrastructure for inclusion in annual risk assessments required under the National Infrastructure Protection Plan. In carrying out this subsection, the Secretary shall coordinate, as appropriate, with the following:

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

"(2) The head of any agency with responsibilities for regulating the critical infrastructure.

"(3) The owners and operators of critical infrastructure, including as a priority, the relevant Critical Infrastructure Partnership Advisory Council entities.

"(4) Any private sector entity determined appropriate by the Secretary.

"(b) EVALUATION OF RISKS.—The Secretary, in coordination with the individuals and entities referred to in subsection (a), shall evaluate the cybersecurity risks iden-

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

''(1) The actual or assessed threat, including a consideration of adversary capabilities and intent, preparedness, target attractiveness, and deterrence capabilities.

''(2) The extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by a disruption, destruction, or unauthorized use of critical infrastructure.

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

''(4) The harm to the economy that would result from the disruption, destruction, or unauthorized use of critical infrastructure.

''(5) Other risk-based security factors that the Secretary, in consultation with the head of the sector specific agency with responsibility for critical infrastructure and the head of any Federal agency that is not a sector specific agency with responsibilities for regulating critical infrastructure, and in consultation with any private sector entity determined appropriate by the Secretary to protect public

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

''(c) AVAILABILITY OF IDENTIFIED RISKS.—The Secretary shall ensure that the risks identified and evaluated under this section for each sector and subsector are made available to the owners and operators of critical infrastructure within each sector and subsector.

''(d) COLLECTION OF RISK-BASED PERFORMANCE STANDARDS.—

''(1) REVIEW AND ESTABLISHMENT.—The Secretary, in coordination with the National Institute of Standards and Technology and the heads of other appropriate agencies, shall review existing internationally recognized consensus-developed risk-based performance standards, including standards developed by the National Institute of Standards and Technology, for inclusion in a common collection. Such collection shall include, for each such risk-based performance standard, an analysis, based on the typical implementation of each performance standard, of each of the following:

''(A) How well the performance standard addresses the identified risks.

''(B) How cost-effective the standard implementation of the performance standard can be.

''(2) USE OF COLLECTION.—The Secretary, in conjunction with the heads of other appropriate agencies, shall develop market-based incentives designed to encourage the use of the collection established under paragraph (1).

''(3) INCLUSION IN REGULATORY REGIMES.—The heads of sector specific agencies with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector specific agency with responsibilities for regulating covered critical infrastructure, in consultation with the Secretary and with any private sector entity determined appropriate by the Secretary, shall propose through notice and comment rulemaking to include the most effective and cost-efficient risk-based performance standards identified in the collection established under paragraph (1) in the regulatory regimes applicable to covered critical infrastructure.

''(e) MITIGATION OF RISKS.—If the Secretary determines that no existing internationally-recognized risk-based performance standard mitigates a risk identified under subsection (a), the Secretary shall—

''(1) collaborate with owners and operators of critical infrastructure and suppliers of technology to develop mitigation strategies for the identified risk, including determining appropriate market-based incentives for the implementation of the identified mitigation; and

''(2) engage with the National Institute of Standards and Technology and appropriate international consensus bodies that develop and strengthen standards and practices to address the identified risk.

''(f) COVERED CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term 'covered critical infrastructure' means any facility or function of a company or government agency that, by way of cyber vulnerability, the destruction or disruption of or unauthorized access to could result in—

''(1) a significant loss of life;

''(2) a major economic disruption, including—

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

''(B) the sustained disruption of financial systems that would lead to long term catastrophic economic damage to the United States;

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

''(4) severe degradation of national security or national security capabilities, including intelligence and defense functions, but excluding military facilities.

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

''(h) REDRESS.—

''(1) IN GENERAL.—Subject to paragraphs (2) and (3), the Secretary shall develop a mechanism, consistent with subchapter II of chapter 5 of title 5, United States Code, for an owner or operator notified under subsection (f) to appeal the identification of a facility or function as covered critical infrastructure under this section.

''(2) APPEAL TO FEDERAL COURT.—A civil action seeking judicial review of a final agency action taken under the mechanism developed under paragraph (1) shall be filed in the United States District Court for the District of Columbia.

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

frastructure shall comply with any requirement of this subtitle relating to covered critical infrastructure until such time as the facility or function is no longer identified as covered critical infrastructure, based on—

''(A) an appeal under paragraph (1);

''(B) a determination of the Secretary unrelated to an appeal; or

''(C) a final judgment entered in a civil action seeking judicial review brought in accordance with paragraph (2).

''SEC. 228. INFORMATION SHARING.

''(a) CYBERSECURITY INFORMATION.—The Secretary shall be responsible for making all cyber threat information, provided pursuant to section 202 of this title, available to appropriate owners and operators of critical infrastructure on a timely basis consistent with the responsibilities of the Secretary to provide information related to threats to critical infrastructures to the organization designated under section 241.

''(b) INFORMATION SHARING.—The Secretary shall, in a timely manner and to the maximum extent possible, consistent with rules for the handling of classified and sensitive but unclassified information, share relevant information regarding cybersecurity threats and vulnerabilities,

and any proposed actions to mitigate them, with all Federal agencies, appropriate State or local government representatives, and appropriate critical infrastructure information systems owners and operators, including by expediting necessary security clearances for designated points of contact for critical infrastructure information systems.

''(c) PROTECTION OF INFORMATION.—The Secretary shall designate, as appropriate, information received from Federal agencies and from critical infrastructure information systems owners and operators and information provided to Federal agencies or critical infrastructure information systems owners and operators pursuant to this section as sensitive security information and shall require and enforce sensitive security information requirements for handling, storage, and dissemination of any such information, including proper protections for personally identifiable information and stripping data of unnecessary identifying information.

"SEC. 229. CYBERSECURITY RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—The Under Secretary for Science and Technology shall support research, development, testing, evaluation, and transition of cybersecurity technology in coordination with a national cybersecurity research and development plan. Such support shall include funda-

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

''(b) ACTIVITIES.—The research and development testing, evaluation, and transition supported under subsection (a) shall include work to—

''(1) advance the development and accelerate the deployment of more secure versions of fundamental Internet protocols and architectures, including for the domain name system and routing protocols;

''(2) improve, create, and advance the research and development of techniques and technologies for proactive detection and identification of threats, attacks, and acts of terrorism before they occur;

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

''(4) improve and create mitigation and recovery methodologies, including techniques and policies

for real-time containment of attacks and development of resilient networks and systems;

''(5) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, test beds, and data sets for assessment of new cybersecurity technologies;

''(6) assist in the development and support of technologies to reduce vulnerabilities in process control systems;

''(7) develop and support cyber forensics and attack attribution;

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

''(9) ensure new cybersecurity technologies are scientifically and operationally validated.

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

''(1) the Under Secretary for National Protection and Programs Directorate; and

''(2) the heads of other relevant Federal departments and agencies, including the National Science Foundation, the Defense Advanced Research

Projects Agency, the Information Assurance Directorate of the National Security Agency, the National Institute of Standards and Technology, the Department of Commerce, academic institutions, the Networking and Information Technology Research and Development Program, and other appropriate working groups established by the President to identify unmet needs and cooperatively support activities, as appropriate.

"SEC. 230. PERSONNEL AUTHORITIES RELATED TO THE OFFICE OF CYBERSECURITY AND COMMUNICATIONS.

''(a) IN GENERAL.—In order to assure that the Department has the necessary resources to carry out the mission of securing Federal systems and critical infrastructure information systems, the Secretary may, as necessary, convert competitive service positions, and the incumbents of such positions, within the Office of Cybersecurity and Communications to excepted service, or may establish new positions within the Office of Cybersecurity and Communications in the excepted service, to the extent that the Secretary determines such positions are necessary to carry out the cybersecurity functions of the Department.

''(b) COMPENSATION.—The Secretary may—

''(1) fix the compensation of individuals who serve in positions referred to in subsection (a) in relation to the rates of pay provided for comparable positions in the Department and subject to the same limitations on maximum rates of pay established for employees of the Department by law or regulations; and

''(2) provide additional forms of compensation, including benefits, incentives, and allowances, that are consistent with and not in excess of the level authorized for comparable positions authorized under title 5, United States Code.

''(c) RETENTION BONUSES.—Notwithstanding any other provision of law, the Secretary may pay a retention bonus to any employee appointed under this section, if the Secretary determines that the bonus is needed to retain essential personnel. Before announcing the payment of a bonus under this subsection, the Secretary shall submit a written explanation of such determination to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

''(d) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section, and annually thereafter, the Secretary shall submit to the Com-

mittee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a detailed report that includes, for the period covered by the report—

''(1) a discussion the Secretary's use of the flexible authority authorized under this section to recruit and retain qualified employees;

''(2) metrics on relevant personnel actions, including—

''(A) the number of qualified employees hired by occupation and grade, level, or pay band;

''(B) the total number of veterans hired;

''(C) the number of separations of qualified employees;

''(D) the number of retirements of qualified employees; and

''(E) the number and amounts of recruitment, relocation, and retention incentives paid to qualified employees by occupation and grade, level, or pay band; and

''(3) long-term and short-term strategic goals to address critical skills deficiencies, including an analysis of the numbers of and reasons for attrition of

employees and barriers to recruiting and hiring individuals qualified in cybersecurity.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 2(b) of such Act is amended by inserting after 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.''.

(c) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing a plan for the execution of the authorities contained in the amendment made by subsection (a).

SEC. 3. NATIONAL INFORMATION SHARING ORGANIZATION.

(a) NATIONAL INFORMATION SHARING ORGANIZATION.—

(1) IN GENERAL.—Title II of the Homeland Security Act of 2002, as amended by section 2, is further amended by adding at the end the following:

"Subtitle E—National Information Sharing Organization

"SEC. 241. ESTABLISHMENT OF NATIONAL INFORMATION SHARING ORGANIZATION.

''(a) ESTABLISHMENT.—There is established a not-for-profit organization for sharing cyber threat information and exchanging technical assistance, advice, and support and developing and disseminating necessary information security technology. Such organization shall be designated as the 'National Information Sharing Organization'.

''(b) PURPOSE.—The National Information Sharing Organization shall serve as a national clearinghouse for the exchange of cyber threat information so that the owners and operators of networks or systems in the private sector, educational institutions, State, tribal, and local governments, entities operating critical infrastructure, and the Federal Government have access to timely and actionable information in order to protect their networks or systems as effectively as possible.

''(c) DESIGNATION.—Not later than 120 days after the date of the enactment of this subtitle, the board of directors established in section 243 shall designate the appropriate organization or organizations as the National Information Sharing Organization.

''(d) CRITERIA FOR DESIGNATION.—The board of directors shall select the organization or organizations to function as the National Information Sharing Organization by taking into consideration the following criteria and other criteria found appropriate by the board:

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

''(2) Whether the organization or organizations have demonstrated the ability to address cyber-related issues in a trusted and cooperative environment maximizing public-private partnerships.

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

''(4) Whether the organization or organizations have an operational center that is open 24 hours a day, seven days a week, and is capable of determining, analyzing, and responding to cyber events.

''(5) Whether the organization or organizations have a proven relationship with the private sector critical infrastructure sectors.

''(6) Whether the organization or organizations have experience implementing privacy protections to

safeguard, sensitive information, including personally identifiable information, in transit and at rest.

"SEC. 242. MISSION AND ACTIVITIES.

"The National Information Sharing Organization shall—

"(1) facilitate the exchange of information, best practices, technical assistance, and support related to the security of public, private, and critical infrastructure information networks and to improve the effectiveness of the National Cyber Incident Response Plan, including by—

"(A) ensuring that the information exchanged shall be stripped of all information identifying the submitter and of any unnecessary personally identifiable information and shall be available to members of the National Information Sharing Organization, including Federal, State, and local government agencies; and

"(B) sharing timely and actionable threat and vulnerability information originating through intelligence collection with appropriate members of the National Information Sharing Organization;

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

''(A) through a secure automated mechanism to be determined by the board; and

''(B) with designated members of the National Information Sharing Organization, including the Federal Government;

''(3) facilitate collaborative research and development projects funded by members of the National Information Sharing Organization to improve the level of cybersecurity in critical infrastructure information systems while maintaining impartiality, the independence of the members of the National Information Sharing Organization, and vendor neutrality;

''(4) develop language to be incorporated into the membership agreement regarding the transferability and use of intellectual property developed by the National Information Sharing Organization and its members under this subtitle ensuring that all members comply with all applicable intellectual property laws; and

''(5) integrate with the Federal Government through the National Cybersecurity and Communica-

tions Integration Center and other existing information sharing and analysis centers, as appropriate.

"SEC. 243. BOARD OF DIRECTORS.

''(a) IN GENERAL.—The National Information Sharing Organization shall have a board of directors which shall be responsible for—

''(1) the executive and administrative operation of the National Information Sharing Organization, including matters relating to funding and promotion of the National Information Sharing Organization; and

''(2) ensuring and facilitating compliance by members of the National Information Sharing Organization with the requirements of this subtitle.

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

''(1) One representative from the Department of Homeland Security.

''(2) Four representatives from three different Federal agencies with significant responsibility for cybersecurity.

''(3) Ten representatives from the private sector, including at least one member representing a small business interest and members representing

each of the following critical infrastructure sectors and subsectors:

''(A) Banking and finance.

''(B) Communications.

''(C) Defense industrial base.

''(D) Energy, electricity subsector.

''(E) Energy, oil, and natural gas subsector.

''(F) Heath care and public health.

''(G) Information technology.

''(H) Water.

''(4) Two representatives from the privacy and civil liberties community.

''(5) The Chair of the National Council of Information Sharing and Analysis Centers.

''(c) INITIAL APPOINTMENT.—Not later than 30 days after the date of the enactment of this subtitle, the Secretary of Homeland Security, in consultation with the heads of the sector specific agencies of the critical infrastructure sectors enumerated in the National Infrastructure Protection Plan, shall appoint the members of the board described under subsection (b)(3) from individuals identified by the sector coordinating councils of the critical infrastructure sectors enumerated in the National Infrastructure Protection Plan.

''(d) TERMS.—

''(1) REPRESENTATIVES OF CERTAIN FEDERAL AGENCIES.—Each member of the board described in subsection (b)(1) and (b)(2) shall be appointed for a term that is not less than one year and not longer than three years from the date of the member's appointment.

''(2) OTHER REPRESENTATIVES.—The original private sector members of the board described subsection (b) shall serve an initial term of one year from the date of appointment under subsection (c), at which time the members of the National Information Sharing Organization shall conduct elections in accordance with the procedures established under subsection (e).

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

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

''(g) SUB-BOARDS.—The board shall have the authority to constitute such sub-boards, or other advisory groups or panels, as may be necessary to assist the board in carrying out its functions under this section. The board shall establish an advisory group made up of the members determined appropriate to participate in the common operation picture described in section 242(2) and to determine information sets, sharing procedures, and operational protocols in creating the common operating picture.

''SEC. 244. CHARTER.

''The board shall develop a charter to govern the operations and administration of the National Information Sharing Organization. The charter shall cover each of the following:

''(1) The organizational structure of the National Information Sharing Organization.

''(2) The governance of the National Information Sharing Organization.

''(3) A mission statement of the National Information Sharing Organization.

''(4) Criteria for membership of the National Information Sharing Organization and for termination of such membership.

''(5) A funding model of the National Information Sharing Organization, including a fee scale that

includes a sliding scale for membership fees for small businesses and promotes broad participation by large, medium, and small business owners and operators of networks or systems in the private sector, entities operating critical infrastructure, educational institutions, State, tribal, and local governments, and the Federal Government.

''(6) Rules for sharing information with members of the National Information Sharing Organization, including the treatment and ownership of intellectual property provided by or to the National Information Sharing Organization, limitations on liability, and consideration of any necessary measures to mitigate anti-trust concerns.

''(7) Technical requirements for participation in the common operating picture and a technical architecture that enables an automated, real-time sharing among members and Federal Government agencies.

''(8) Rules for participating in collaborative research and development projects.

''(9) Protections of privacy and civil liberties to be used by the National Information Sharing Organization and its members, including appropriate measures—

''(A) for public transparency and oversight;

''(B) to ensure that only cyber threat information is shared with and by the National Information Sharing Organization; and

''(C) to omit personally identifiable information not necessary to describe a cyber threat from information shared with and by the National Information Sharing Organization.

''(10) Security requirements and member obligations for the protection of information from other sources, including private and governmental.

''(11) Procedures for coordinating cooperative research and development projects funded by members of the National Information Sharing Organization with the Science and Technology Directorate and the Networking and Information Technology Research and Development Program.

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

''(13) Procedures for the incorporation of international entities and allied government agencies into the membership of the National Information Sharing Organization.

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

''SEC. 245. MEMBERSHIP.

''Not later than 90 days after the date of the enactment of this subtitle, the board of directors of the National Information Sharing Organization shall establish criteria procedures for the voluntary membership by State and local government departments, agencies, and entities, private sector businesses and organizations, and academic institutions in the National Information Sharing Organization.

''SEC. 246. FUNDING.

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

''SEC. 247. CLASSIFIED INFORMATION.

''Consistent with the protection of sensitive intelligence sources and methods, the Secretary, in conjunction with the heads of appropriate Federal agencies, shall facilitate, through the National Cybersecurity and Communications Integration Center—

''(1) the sharing of classified cybersecurity threat information in the possession of a Federal

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

''(2) the declassification and sharing of cybersecurity threat information in the possession of a Federal agency related to threats to information networks with members of the National Information Sharing Organization.

''SEC. 248. VOLUNTARY INFORMATION SHARING.

''(a) IN GENERAL.—

''(1) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider may, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity.

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

''(A) share cyber threat information with the National Information Sharing Organization

and its membership, including the Federal Government; or

''(B) authorize their cybersecurity provider to share cyber threat information on their behalf with the National Information Sharing Organization and its membership, including the Federal Government.

''(3) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

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

''(B) share such cyber threat information with the National Information Sharing Organization and its membership, including the Federal Government.

''(b) USES OF SHARED INFORMATION.—Notwithstanding any other provision of law, information shared with or provided to the National Information Sharing Organization or to a Federal agency or private entity through the National Information Sharing Organization by any member of the National Information Sharing Organization that is not a Federal agency in furtherance of

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

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

''(2) shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal agency, any other Federal, State, tribal, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted to the National Information Sharing Organization for the purpose of facilitating the missions of such Organization, as articulated in the mission statement required under section 244;

''(3) shall not be used or disclosed by any officer or employee of the United States for purposes other than a cybersecurity purpose, including any regulatory purpose, except—

''(A) to further an investigation or the prosecution of a cybersecurity related criminal act; or

''(B) to disclose the information to the appropriate congressional committee;

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

''(A) be made available pursuant to any State or local law requiring disclosure of information or records;

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

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

''(5) shall not, if subsequently provided to a private entity, be used for any purpose other than a cybersecurity purpose;

''(6) does not constitute a waiver of any applicable privilege or protection provided under law, such as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain; and

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

for a failure to warn or disclose provided that the information is shared with the Federal Government through the National Information Sharing Organization in accordance with the procedures established under this section.

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

''(d) PROCEDURES.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this subtitle, the board of directors of the National Information Sharing Organization shall establish uniform procedures for the receipt, care, and storage of information that is voluntarily submitted to the Federal Government through the National Information Sharing Organization.

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

''(A) the acknowledgment of receipt by the National Information Sharing Organization of cyber threat information that is voluntarily submitted to the National Information Sharing Organization;

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

''(C) the care and storage of such information;

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

''(E) the protection of the privacy rights and civil liberties of any individuals who are subjects of such information; and

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

''(e) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or other-

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

''(1) to obtain or disseminate cyber threat information in a manner other than through the National Information Sharing Organization; and

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

''(f) DEFINITIONS.—In this section:

''(1) The term 'cyber attack' means the intentional use of a wire or electronic communication to access or attempt to access without authorization or in excess of authorization a protected computer in a manner that subverts a technical control and in so doing—

''(A) causes or attempts to cause the modification, destruction, or disclosure of information;

''(B) causes or attempts to cause damage and loss; or

''(C) renders or attempts to render information in a protected computer, or the computer itself, unavailable.

''(2) The term 'cybersecurity related criminal act' means conduct that is already a crime under Federal or State law that involves—

''(A) efforts to degrade, disrupt or destroy a cybersecurity system or network; or

''(B) theft or misappropriation of private or government information, intellectual property or personally identifiable information from an information system or network.

''(3) The term 'cybersecurity provider' means a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes.

''(4) The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

''(A) efforts to degrade, disrupt or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(5) The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguarding, a

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

''(A) efforts to degrade, disrupt or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(6) The term 'cyber threat information' means the information—

''(A) that is necessary to identify or describe—

''(i) a method of defeating a technical or operational control that corresponds to a cyber attack;

''(ii) a method of causing a person with authorized access to an information system or to information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control;

''(iii) information exfiltrated in a cyber attack when such information necessary to identify or describe the attack;

''(iv) anomalous patterns of communications that appear to be transmitted in

connection with a cyber attack, but does not include other communications content, or dialing, routing, addressing and signaling information not necessary to describe such attack;

''(v) anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information to be used in a cyber attack; or

''(vi) a method for remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system associated with a known or suspected cyber attack; and

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

''(7) The term 'technical control' means a hardware or software restriction on access or use of a protected computer or information in a protected computer that is intended to ensure the confidentiality, integrity, or availability of that computer or information.

''(8) The term 'protected entity' means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

''(9) The term 'self-protected entity' means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

''SEC. 249. ANNUAL INDEPENDENT AUDITS.

''The board of directors of the National Information Sharing Organization shall commission, on an annual basis, an audit by a qualified, independent auditing firm approved by the Secretary, to review the compliance of the National Information Sharing Organization and its members with the information sharing rules set forth in section 248 and the information sharing rules established by the board pursuant to the National Information Sharing Organization charter required under section 244. Such audit—

''(1) shall identify instances in which information may have been shared in a manner inconsistent with procedures required under section 248 or with the information sharing rules established by the board pursuant to section 244, with the National Information Sharing Organization, with members of the National Information Sharing Organization, or

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

''(2) shall be provided to the Secretary and to the Committee on Homeland Security of the House of Representatives and to the Homeland Security and Governmental Affairs Committee of the Senate;

''(3) shall be made public, with appropriate redactions to protect the identity of National Information Sharing Organization members; and

''(4) may include a classified annex.

''SEC. 250. PENALTIES.

''(a) IN GENERAL.—It shall be unlawful for any officer, employee, representative, or agent of the United States or of any Federal agency, or any employee or officer of the National Information Sharing Organization, its member entities, and any representatives or agents of the National Information Sharing Organization or its member entities to knowingly publish, divulge, disclose, or make known in any manner or to any extent not authorized by law, any cyber threat information protected from disclosure by this title coming to such officer or employee in the course of the employee's employment or official duties or by reason of any examination or investigation made by,

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

''(b) PENALTY.—Any person who violates subsection (a) shall be fined under title 18, United States Code, imprisoned for not more than one year, or both, and shall be removed from office or employment.

''SEC. 251. AUTHORITY TO ISSUE WARNINGS.

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

''(1) the source of any voluntarily submitted information that forms the basis for the advisory, alert, or warning; and

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

''SEC. 252. EXEMPTION FROM ANTITRUST PROHIBITIONS.

''The exchange of information by and between private sector members of the National Information Sharing Organization in furtherance of the mission and activities of the National Information Sharing Organization shall not

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

"SEC. 253. LIMITATION.

"(a) NO APPROPRIATIONS.—For any fiscal year after fiscal year 2015, no Federal appropriations shall be authorized for the National Information Sharing Organization.

"(b) MEMBERSHIP FEES FOR FEDERAL AGENCIES.—Membership fees for the National Information Sharing Organization shall not be collected from the Federal Government for any fiscal year prior to fiscal year 2015 and the Federal Government shall not be assessed a fee in excess of the fee collected from the largest private sector member of the National Information Sharing Organization.' ''.

(2) CLERICAL AMENDMENT.—The table of contents in section 2(b) of such Act, as amended by section 2, is further amended by adding at the end of 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.

(b) INITIAL EXPENSES.—There is authorized to be appropriated $10,000,000 for each of fiscal years 2013, 2014, and 2015 for initial expenses associated with the establishment of the National Information Sharing Organization under subtitle E of title II of the Homeland Security Act of 2002, as added by subsection (a). Such amounts shall be derived from amounts appropriated for the operations of the Management Office for the Directorate of Science and Technology of the Department of Homeland Security.

SEC. 4. REPORT ON SUPPORT FOR REGIONAL CYBERSECURITY COOPERATIVES.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the Secretary's plan to provide support to regional, State, and local grassroots cyber cooperatives designed to decrease cyber disruptions to critical infrastructure, increase cyber workforce training efforts, increase community awareness of cybersecurity, organize community cyber-emergency preparedness efforts, build resiliency of regional, State, and local critical services, and coordi-

nate academic technical and policy research effort. The report shall include each of the following:

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

(2) Recommendations for integrating regional, State, and local grassroots cyber cooperatives in regional, State, and Federal cyber disruption plans.

(3) A plan for increasing cyber threat information sharing between regional, State, and local cyber cooperatives, the Federal Emergency Management Agency, the Department of Homeland Security, and the National Information Sharing Organization.

(4) A plan to promote with the National Information Sharing Organization a ground up, community-based network of cyber cooperatives.

(5) A plan for establishing a Federal online portal for existing groups to coordinate online training, best practices, and other cybersecurity integration efforts.

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

SEC. 5. PILOT PROGRAM ON CYBERSECURITY TRAINING FOR FUSION CENTERS.

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

(b) PILOT PROGRAM.—

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

(2) CURRICULUM AND PERSONNEL.—In creating the curriculum for the training program and conducting the program, the Secretary may assign personnel from the Department of Homeland Security, including personnel from the Office of Cybersecurity and Communications.

SEC. 6. ASSESSMENT OF SECTOR BY SECTOR CYBERSECURITY PREPAREDNESS.

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

operators of critical infrastructure through the Critical Infrastructure Partnership Advisory Council, and in consultation with the sector specific agencies and agencies with regulatory authority over critical infrastructure, and other appropriate organizations shall conduct an assessment of the cybersecurity preparedness of each sector of the critical infrastructure as described in the National Infrastructure Protection Plan. Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees the results and recommendations of that assessment in an unclassified report, with a classified annex if appropriate.

(b) CONTENTS OF REPORT.— The report required by subsection (a) shall include an assessment of the current state of the cybersecurity preparedness of each sector, including an evaluation of—

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

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

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

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

(4) the current state of cybersecurity recovery planning and capability for each sector, an articulation of what an adequate level of recovery planning and capability should be for the sector, and recommendations for how and over what time frame the gap should be closed between current and desired end-state.

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