IB

Union Calendar No. 501

112TH CONGRESS
2D SESSION

H. R. 3674

[Report No. 112–592, Part I]

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

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 15, 2011

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

JULY 11, 2012

Reported from the Committee on Homeland Security with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

JULY 11, 2012

The Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and the Permanent Select Committee on Intelligence discharged; referred to the Committee on Energy and Commerce for a period ending not later than September 21, 2012, for consideration of such provisions of the bill and amendment as fall within the jurisdiction of that committee pursuant to clause 1(f) of rule X.

SEPTEMBER 21, 2012

Additional sponsor: Mr. MEEHAN

SEPTEMBER 21, 2012

Deleted sponsor: Mr. LANGEVIN (added December 15, 2011; deleted April 25, 2012)

SEPTEMBER 21, 2012

The Committee on Energy and Commerce discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on December 15, 2011]

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2012" or the "PRECISE Act of 2012".

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. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY ACTIVITIES.

"(a) IN GENERAL.—The Secretary shall perform necessary activities to help facilitate the protection of Federal systems and, solely upon the request of critical infrastructure owners and operators, assist such critical infrastructure owners and operators in protecting their critical infrastructure information systems to include—

"(1) conduct risk assessments, subject to the availability of resources and, solely upon request from critical infrastructure owners and operators, critical infrastructure information systems;

"(2) assist in fostering the development, in conjunction with the National Institute of Standards and

Technology and other Federal departments and agencies 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) assist in efforts to mitigate communications and information technology supply chain vulnerabilities;

"(4) support nationwide awareness and outreach efforts, to include participation in appropriate interagency cybersecurity awareness and education programs, to educate the public;

"(5) conduct exercises, simulations, and other activities designed to support and evaluate the national cyber incident response plan; and

"(6) subject to the availability of resources and, upon request of critical infrastructure owners and operators, provide technical assistance, including sending on-site teams, to such critical infrastructure owners and operators.

"(b) INTERAGENCY DUTIES.—At the direction of the Office of Management and Budget pursuant to subchapter II of chapter 35 of title 44, United States Code, the Secretary shall—

"(1) conduct targeted risk assessments and operational evaluations, in conjunction with the heads of other agencies, for Federal systems that may include threat, vulnerability, and impact assessments and penetration testing;

"(2) in conjunction with the National Institute of Standards and Technology and appropriate Federal departments and agencies, as well as the private sector, provide for the use of consolidated intrusion detection, prevention, or other protective capabilities and use associated countermeasures for the purpose of protecting Federal systems from cybersecurity threats;

"(3) in conjunction with other agencies and the private sector, assess and foster the development of information security technologies and capabilities for use and dissemination throughout the Department of Homeland Security and to be made available across multiple agencies;

"(4) designate an entity within the Department of Homeland Security to receive reports and information about cybersecurity incidents, threats, and vulnerabilities affecting Federal systems; and

"(5) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance for Federal systems.

"(c) CYBERSECURITY OPERATIONAL ACTIVITY.—

"(1) IN GENERAL.—While carrying out the responsibilities authorized in paragraphs (2) and (3) of subsection (b), the Secretary is authorized, notwithstanding any other provision of law, to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on Federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes if the Secretary certifies that—

"(A) such acquisitions, interceptions, and countermeasures are reasonably necessary for the purpose of protecting Federal systems from cybersecurity threats;

"(B) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected cybersecurity threat and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;

"(C) information obtained pursuant to activities authorized under this subsection will only be retained, used, or disclosed to protect

Federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed;

"(D) notice has been provided to users of Federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and

"(E) such activities are implemented pursuant to policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications and other system traffic that have been reviewed and approved by the Attorney General.

"(2) OBTAINING ASSISTANCE.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic consistent with paragraph (1).

"(3) PERMISSION BY OTHER AGENCIES.—Agencies are authorized to permit the Secretary, or a private entity providing assistance to the Secretary under paragraph (2), to acquire, intercept, retain, use, or disclose communications, system traffic, records, or other information transiting to or from or stored on a Federal system, notwithstanding any other provision of law, for the purpose of protecting Federal systems from cybersecurity threats or mitigating such threats in connection with activities under this subsection.

"(4) PRIVILEGED COMMUNICATIONS.—No otherwise privileged communication obtained in accordance with, or in violation of, this subtitle shall lose its privileged character.

"(d) COORDINATION.—

"(1) COORDINATION WITH OTHER ENTITIES.—In carrying out cybersecurity activities subsection (a), the Secretary shall coordinate, as appropriate, with—

"(A) the head of relevant Federal departments or agencies;

"(B) representatives of State and local governments;

"(C) owners and operators of critical infrastructure;

"(D) suppliers of technology for owners and operators of critical infrastructure;

"(E) academia; and

"(F) international organizations and foreign partners.

"(2) LEAD DHS CYBERSECURITY OFFICIAL.—The Secretary shall designate a lead cybersecurity official within the Department 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.

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

"(e) STRATEGY.—In carrying out the cybersecurity activities of the Department under subsection (a), the Secretary shall develop and maintain a strategy that—

"(1) articulates the actions of the Department that are necessary to assure the readiness, reliability,

continuity, integrity, and resilience of Federal systems and critical infrastructure information systems;

"(2) includes explicit goals and objectives for the Department as well as specific timeframes for achievement of stated goals and objectives by the Department;

"(3) fosters the continued superiority and reliability of the United States information technology and communications sectors; and

"(4) ensures that activities of the Department are undertaken in a manner that protects statutory privacy rights and civil liberties of United States persons.

"(f) NO RIGHT OR BENEFIT.—The provision of assistance or information to critical infrastructure owners and operators, upon request of such critical infrastructure owners and operators, 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 critical infrastructure owner or and operator pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other critical infrastructure owner or and operator.

"(g) PRIVACY OFFICER OVERSIGHT.—The Privacy Officer of the Department of Homeland Security shall review

on an ongoing basis, and prepare, as necessary, privacy impact assessments on, the cybersecurity policies, programs, and activities of the Department of Homeland Security for such purposes as ensuring compliance with all relevant constitutional and legal protections.

"(h) SAVINGS CLAUSE.—Nothing in this subtitle shall be interpreted to—

"(1) alter or amend the authorities of any Federal department or agency other than the Department of Homeland Security, including the law enforcement or intelligence authorities of any such Federal department or agency or the authority of any such Federal department or agency to protect sources and methods and the national security;

"(2) limit or modify an existing information sharing or other relationship;

"(3) prohibit a new information sharing or other relationship;

"(4) require a new information sharing or other relationship between the Federal Government and a private sector entity;

"(5) alter or otherwise limit the authority of any Federal department or agency to also undertake any activities that the Department of Homeland Security is authorized to undertake pursuant to this section; or

"(6) provide additional authority to, or modify an existing authority of the Department of Homeland Security to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

"(i) DEFINITIONS.—In this section:

"(1) The term 'countermeasure' means automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats.

"(2) The term 'Federal systems' means information systems owned, operated, leased, or otherwise controlled by a Federal department or agency, or on behalf of a Federal department or agency, except for national security systems or those information systems under the control of, used by, or storing information of the Department of Defense or any element of the Intelligence Community, including any information systems used or operated by a contractor of the Department of Defense or any element of the Intelligence Community, or other organization on behalf

of the Department of Defense or any element of the Intelligence Community.

"(3) The term 'critical infrastructure information systems' means any information system 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.

"(4) The term 'information system' means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

"(A) computers and computer networks;

"(B) ancillary equipment;

"(C) software, firmware, and related procedures;

"(D) services, including support services; and

"(E) related resources.

"(5) The term 'national security system' means any information infrastructure (including any telecommunications system) used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency—

"(A) the function, operation, or use of which—

"(i) involves intelligence activities or intelligence-related activities;

"(ii) involves cryptologic activities related to national security;

"(iii) involves command and control of military forces;

"(iv) involves equipment that is an integral part of a weapon or weapons system; or

"(v) is critical to the direct fulfillment of military or intelligence missions;

"(B) that contains information related to the activities and other matters set forth in subparagraph (A); or

"(C) that is protected by procedures established for classified, national security, foreign policy, intelligence or intelligence-related, or other appropriate information.

"SEC. 227. 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 set forth in section 226, 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 appropriate Congressional committees 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.

"SEC. 228. FEDERAL PREEMPTION, EXCLUSIVITY, AND LAW ENFORCEMENT AND INTELLIGENCE ACTIVITIES.

"(a) PREEMPTION.—This subtitle supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates the acquisition, interception, retention, use, or disclosure of communications, records, or other information by private entities or governmental entities to the extent such statute is inconsistent with this subtitle.

"(b) ADDITIONAL EXCLUSIVE MEANS.—Section 226(c) constitutes an additional exclusive means for the domestic

interception of wire or electronic communications, in accordance with the provisions of law codified at section 1812(b) of title 50, United States Code.

''(c) LIMITATION.—This subtitle does not authorize the Secretary to engage in law enforcement or intelligence activities that the Department is not otherwise authorized to conduct under existing law.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 225 the following new items:

''Sec. 226. Department of Homeland Security cybersecurity activities.
''Sec. 227. Personnel authorities related to the Office of Cybersecurity and Communications.
''Sec. 228. Federal preemption, exclusivity, and law enforcement and intelligence activities.''.

(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. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY INFORMATION SHARING.

(a) DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY INFORMATION SHARING.—

(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—Department of Homeland Security Cybersecurity Information Sharing

"SEC. 241. INFORMATION SHARING.

"The Secretary shall make appropriate cyber threat information obtained by the Department pursuant to title XI of the National Security Act of 1947 or other information appropriately in the possession of the Department available to appropriate owners and operators of critical infrastructure on a timely basis consistent with the statutory and other appropriate restrictions on the dissemination of such information and with the responsibilities of the Secretary under this title.

"SEC. 242. ESTABLISHMENT OF NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

"(a) ESTABLISHMENT.—There is established within the Department the National Cybersecurity and Communications Integration Center.

"(b) PURPOSE.—The center established pursuant to subsection (a) shall be the primary entity within the Department for sharing timely cyber threat information and

exchanging technical assistance, advice, and support with appropriate entities pursuant to the Department's authorities.

"SEC. 243. BOARD OF ADVISORS.

"(a) IN GENERAL.—The National Cybersecurity and Communications Integration Center shall have a board of advisors which shall advise the Secretary on the efficient operation of the National Cybersecurity and Communications Integration Center.

"(b) COMPOSITION.—The board shall be composed of 13 members, including the following:

"(1) Eleven representatives from the critical infrastructure sectors enumerated in the National Infrastructure Protection Plan, of which at least one member shall represent a small business interest and at least one member shall represent each of the following sectors:

"(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.

"(I) Chemical.

"(2) Two representatives from the privacy and civil liberties community.

"(3) 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) from individuals identified by the sector coordinating councils of the critical infrastructure sectors enumerated in the National Infrastructure Protection Plan.

"(d) TERMS.—

"(1) CRITICAL INFRASTRUCTURE REPRESENTATIVES.—Each member of the board described in subsection (b)(1) 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, as determined by the member's sector coordinating council.

"(2) OTHER REPRESENTATIVES.—Each member of the board described in subsection (b)(2) or (3) shall serve an initial term that is not less than two years

and not longer than three years from the date of the member's appointment, and each such member shall select the member's successor.

"(e) DUTIES.—The board shall—

"(1) meet not less frequently than quarterly;

"(2) act as an advocate on behalf of the private sector in improving the operations of the National Cybersecurity Communications Integration Center; and

"(3) submit to the Secretary and the appropriate committees of Congress the annual report described in section 247.

"(f) ACCESS TO INFORMATION.—The members of the board shall, subject to the laws and procedures applicable to national security background investigations and security clearances, be provided with the appropriate security clearances and have access to appropriate information shared with the National Cybersecurity and Communications Integration Center and shall be subject to all of the limitations on the use of such information.

"(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.

"SEC. 244. CHARTER.

"The Secretary shall develop a charter to govern the operations and administration of the National Cybersecurity and Communications Integration Center consistent with the requirements of title XI of the National Security Act of 1947. The charter shall include each of the following:

"(1) The organizational structure of the National Cybersecurity and Communications Integration Center, including a delineation of the mission expectations and responsibilities of the various elements assigned to the Center.

"(2) A mission statement of the National Cybersecurity and Communications Integration Center.

"(3) A plan that 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.

"(4) Procedures for making appropriate cyber incident information available to outside groups for academic research and insurance actuarial purposes.

"SEC. 245. PARTICIPATION.

"Not later than 90 days after the date of the enactment of this subtitle, the Secretary shall publish the criteria and procedures for voluntary participation and voluntary phys-

ical collocation by appropriate Federal, State and local government departments, agencies and entities, and private sector businesses and organizations within the National Cybersecurity and Communications Integration Center.

"SEC. 246. ANNUAL REPORT.

"The board of advisors of the National Cybersecurity Communications Integration Center shall submit to the Secretary and the appropriate committees of Congress an annual report on the status of the National Cybersecurity Communications Integration Center and how the Center accomplished its purpose under section 242 during the year covered by the report. Each such report shall include, for the year covered by the report—

"(1) information on the amount and nature of information shared by and through the Center;

"(2) the number of violations of statutory information sharing restrictions and the procedures established for the Center and any steps taken by the Center to reduce and eliminate such violations;

"(3) any changes to the Center's charter as agreed upon by the board and the membership; and

"(4) proposed ways to improve information sharing by and through the Center.

"SEC. 247. AUTHORITY TO ISSUE WARNINGS.

"The Secretary may, in coordination with appropriate Federal departments and agencies, provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential cybersecurity threats as appropriate. In issuing such an advisory, alert, or warning, the Secretary shall not disclose—

"(1) without the express consent of an entity voluntarily sharing information with the Federal Government pursuant to title XI of the National Security Act of 1947 and the Federal department or agency that initially received such information, any such information that forms the basis for the advisory, alert, or warning or the source of such information;

"(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; and

"(3) any information that is restricted by statute, rule, or regulation, including information restricted from disclosure under title XI of the National Security Act of 1947, and information relating to sources and methods and the national security of the United States.

"SEC. 248. DEFINITIONS.

"In this subtitle:

"(1) CYBER THREAT INFORMATION.—The term 'cyber threat information' means the information directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

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

"(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

"(2) CYBERSECURITY THREAT.—The term 'cybersecurity threat' means a vulnerability of, or threat to, a system or network of a government or private entity, including—

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

"(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

"SEC. 249. SAVINGS CLAUSE.

"Nothing in this subtitle shall be interpreted to—

"(1) alter or amend the authorities of any Federal department or agency other than the Department of Homeland Security, including the law enforcement or intelligence authorities of any such Federal department or agency or the authority of any such Federal department or agency to protect sources and methods and the national security;

"(2) limit or modify an existing information sharing or other relationship;

"(3) prohibit a new information sharing or other relationship;

"(4) require a new information sharing or other relationship between the Federal Government and a private sector entity;

"(5) alter or otherwise limit the authority of any Federal department or agency to also undertake any activities that the Department of Homeland Security is authorized to undertake pursuant to this section; or

"(6) provide additional authority to, or modify an existing authority of the Department of Homeland Security to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(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:

(b) AUTHORIZATION OF APPROPRIATION FOR THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.—There is authorized to be appropriated $4,000,000 for each of fiscal years 2013, 2014, and 2015 for the administration and management of the National Cybersecurity and Communications Integration Center.

SEC. 4. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—Title III of the Homeland Security Act of 2002 is amended by adding at the end the following:

"SEC. 318. 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. Such support shall include fundamental, long-term research to improve the ability of the United States to prevent, pro-

tect 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 develop-

ment 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;

"(9) ensure new cybersecurity technology is scientifically and operationally validated; and

"(10) facilitate the planning, development, and implementation of international cooperative activities (as defined in section 317) to address cybersecurity and energy infrastructure with foreign public or private entities, governmental organizations, businesses (including small business concerns and social and economically disadvantaged small business concerns (as those terms are defined in sections 3 and 8 of the Small Business Act (15 U.S.C. 632 and 637) respectively)), federally funded research and development centers and universities from countries that may include Israel, the United Kingdom, Canada, Australia,

Singapore, Germany, New Zealand, and other allies, as determined by the Secretary, in research and development of technologies, best practices, and other means to protect critical infrastructure, including the national electric grid.

"(c) COORDINATION.—In carrying out this section, the Under Secretary shall coordinate all 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.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 2 and 3, is further amended by inserting after the item relating to section 317 the following new item:

"Sec. 318. Cybersecurity research and development.".

SEC. 5. REPORT ON SUPPORT FOR REGIONAL CYBERSECURITY COOPERATIVES.

(a) IN GENERAL.—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 what support, if any, the Department of Homeland Security might provide to regional, State, and local grassroots cyber cooperatives.

(b) CONTENTS.—The report shall include an analysis of the progress in establishing the "NET Guard" authorized under section 224 of the Homeland Security Act of 2002 (6 U.S.C. 144) to build a national technology guard for cyber response capabilities and an assessment of whether a grant process for pilot regional, State, or local cyber cooperatives would be beneficial. Such assessment should—

(1) evaluate whether the grant process should include a methodology of identifying recognized national experts in relevant areas of science and technology, including agreed upon metrics measuring the expertise and demonstrated capabilities of such experts; and

(2) address the following:

(A) The appropriateness of the establishment and maintenance of a national volunteer

experts registry system comprised of the demonstrated national experts described in this paragraph, together with information relating to their particular areas of expertise and who may be called upon to respond to a cyber incident.

(B) The need to identify and leverage existing capabilities of cyber response and cyber workforce challenge programs in States, local governments, private sector entities, and nonprofit organizations to potentially accelerate the implementation of the NET Guard.

(C) The requirements for the implementation of a plan to improve national capability with minimum descriptions of the following:

(i) How to evaluate the demonstrated national experts in relevant areas of science and technology.

(ii) How to establish and maintain the national volunteer experts registry system.

(iii) Potential funding models incorporating private sector funding.

SEC. 6. CYBERSECURITY DOMESTIC PREPAREDNESS CONSORTIUM AND CYBERSECURITY TRAINING CENTER.

(a) CYBERSECURITY DOMESTIC PREPAREDNESS CONSORTIUM.—

(1) IN GENERAL.—The Secretary of Homeland Security may establish a consortium to be known as the "Cybersecurity Domestic Preparedness Consortium".

(2) FUNCTIONS.—The Consortium established under paragraph (1) may—

(A) provide training to State and local first responders and officials specifically for preparing and responding to cybersecurity attacks;

(B) develop and update a curriculum utilizing the DHS National Cyber Security Division sponsored Community Cyber Security Maturity Model (CCSMM) for State and local first responders and officials;

(C) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response; and

(D) conduct cybersecurity training and simulation exercises to defend from and respond to cyber attacks.

(3) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that develop, update, and deliver cybersecurity training in support of homeland security.

(b) CYBERSECURITY TRAINING CENTER.—As a part of the Cybersecurity Domestic Preparedness Consortium, the Secretary may establish where appropriate one or more cybersecurity training centers to provide training courses and other resources for State and local first responders and officials to improve preparedness and response capabilities.

(c) PLAN FOR FUSION CENTERS.—The Cybersecurity Domestic Preparedness Consortium shall develop a plan to implement as one of the Cybersecurity Training Centers 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.

(d) 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.

(3) COORDINATION.—The curriculum for the training and for conducting the program will be coordinated with that of the Cyber Security Domestic Preparedness Consortium.

SEC. 7. SAVINGS CLAUSE.

Nothing in this Act shall be interpreted to—

(1) alter or amend the authorities of any Federal department or agency other than the Department of Homeland Security, including the law enforcement or intelligence authorities of any such Federal department or agency or the authority of any such Federal department or agency to protect sources and methods and the national security;

(2) alter or otherwise limit the authority of any Federal department or agency to also undertake any activities that the Department of Homeland Security is authorized to undertake pursuant to this section; or

(3) provide additional authority to, or modify an existing authority of the Department of Homeland

Security to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

Union Calendar No. 501

112TH CONGRESS
2D SESSION

H. R. 3674

[Report No. 112–592, Part I]

A BILL

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

SEPTEMBER 21, 2012

The Committee on Energy and Commerce discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed