AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

112TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 112–592
Part 1

PROMOTING AND ENHANCING CYBERSECURITY AND INFORMATION SHARING EFFECTIVENESS ACT OF 2012

JULY 11, 2012.—Ordered to be printed

Mr. KING of New York, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 3674]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3674) to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

19–006

The amendment is as follows:

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 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 Com-

mittee 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 subboards, 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 physical 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:

"Subtitle E—Department of Homeland Security Cybersecurity Information Sharing

"Sec. 241. Information sharing.
"Sec. 242. Establishment of National Cybersecurity and Communications Integration Center.
"Sec. 243. Board of advisors.
"Sec. 244. Charter.
"Sec. 245. Participation.
"Sec. 246. Annual report.
"Sec. 247. Authority to issue warnings.
"Sec. 248. Definitions.
"Sec. 249. Savings clause.".

(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, 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;

"(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 non-profit 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.

PURPOSE AND SUMMARY

The purpose of H.R. 3674 is to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security's cybersecurity mission has never been authorized by statute. This bill authorizes the Department to conduct its cybersecurity mission, establishes the National Cybersecurity and Communications Integration Center to serve as a National clearinghouse for the exchange of cyber threat information, and designates the Department as a focal point for cybersecurity for both the civilian Federal Government as well as private sector critical infrastructure owners and operators. The Department has expressed that it has difficulty hiring qualified personnel to perform the cybersecurity mission, the process does not provide enough speed or flexibility to make the Department competitive in the employment market. Therefore, the bill also provides hiring flexibility similar to authority previously granted to the Secretary of Defense to assist in hiring qualified and capable employees to engage in the cybersecurity mission. The Committee recognizes that more work remains to be done to secure cyber networks and enhance coordination between the Department of Homeland Security and the private sector in assessing risk and implementing cyber security standards.

HEARINGS

During the 112th Congress, the Committee held numerous hearings on cybersecurity issues and legislative proposals. The hearings are detailed below.

On March 16, 2011 the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Examining the Cyber Threat to Critical Infrastructure and the American Economy." The Subcommittee received testimony from Hon. Phillip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; Dr. Phyllis Schneck, Vice President and Chief Technical Officer, McAfee Inc.; Mr. James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies; and Ms. Mischel Kwon, President, Mischel Kwon Associates.

On April 15, 2011 the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure." The Subcommittee received testimony from Mr. Sean McGurk, Director, National Cybersecurity and

Communications Integration Center, Department of Homeland Security; Mr. Gerry Cauley, President and CEO, North American Electric Reliability Corporation; Ms. Jane Carlin, Chair, Financial Services Sector Coordinating Council; and Mr. Edward Amoroso, Senior Vice President and Chief Security Officer, AT&T.

On June 24, 2011, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal." The Subcommittee received testimony from Ms. Melissa Hathaway, President, Hathaway Global Strategies, LLC; Dr. Greg Shannon, Chief Scientist for Computer Emergency Readiness Team, Software Engineering Institute, Carnegie Mellon University; Mr. Leigh Williams, BITS President, The Financial Services Roundtable; and Mr. Larry Clinton, President, Internet Security Alliance.

On October 6, 2011 the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Cloud Computing: What are the Security Implications?" The Subcommittee received testimony from Hon. Richard Spires, Chief Information Officer, U.S. Department of Homeland Security; Dr. David McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration; Mr. Greg Wilshusen, Director of Information Security Issues, Government Accountability Office; Mr. James W. Sheaffer, President, North American Public Sector, Computer Sciences Corporation; Mr. Timothy Brown, Senior Vice President, and Chief Architect for Security, CA Technologies; Mr. James R. Bottum, Vice Provost for Computing & Information Technology, and Chief Information Officer, Clemson University; and Mr. John Curran, Chief Executive Officer, American Registry of Internet Numbers.

On December 6, 2011 the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Hearing on Draft Legislative Proposal on Cybersecurity." The Subcommittee received testimony from Ms. Cheri McGuire, Vice President of Global Government Affairs and Cybersecurity Policy, Symantec Corporation; Dr. Greg Shannon, Chief Scientist for Computer Emergency Readiness Team, Software Engineering Institute, Carnegie Mellon University; Mr. Gregory T. Nojeim, Senior Counsel and Director, Project on Freedom, Security & Technology, Center for Democracy & Technology; and Mr. Kevin R. Kosar, Analyst in American Government, Congressional Research Service.

COMMITTEE CONSIDERATION

Subcommittee Consideration

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on February 1, 2012, and ordered H.R. 3674 reported to the Full Committee for consideration, with a favorable recommendation, amended, by voice vote. The Subcommittee took the following actions:

The Subcommittee adopted H.R. 3674, as amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. LUNGREN (#1) was AGREED TO, by voice vote.

An amendment to the Amendment in the Nature of a Substitute offered by MS. RICHARDSON (#1A) ; was AGREED TO by unanimous consent.

Page 6. Line 22, strike "and" the second place it appears.

Page 6, after line 22, insert a new paragraph (11) and redesignate accordingly.

An amendment to the Amendment in the Nature of a Substitute offered by MR. LONG (#1B); was AGREED TO by unanimous consent.

Page 18, line 3, strike "and".

Page 18, line 4, after "operators" insert the following ", Information Sharing and Analysis Centers, appropriate academic and private sector entities that conduct cybersecurity or information security research and development, and appropriate private sector entities that provide cybersecurity or information security products or services."

Page 18, line 6, strike "critical infrastructure information systems" and insert "all appropriate entities".

An amendment to the Amendment in the Nature of a Substitute offered by MR. LONG (#1C); was AGREED TO by unanimous consent.

Page 20, line 16, strike "and".

Page 20, line 18, strike the period and insert "; and".

Page 20, after line 18, insert a new paragraph (10).

An amendment to the Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1D); was AGREED TO by unanimous consent.

Page 54, line 22, insert a new section entitled "Sec. 7. Report on Foreign Entities Posing Cybersecurity Threats to Critical Infrastructure."

An amendment to the Amendment in the Nature of a Substitute offered by MR. LONG (#1E); was AGREED TO by unanimous consent.

Page 47, after line 11, insert the following (and renumber the subsequent sections proposed to be inserted in the Homeland Security Act of 2002 by section 3 accordingly and conform the proposed amendment to the table of contents beginning on page 49, line 17):

A new section "Sec. 250. Annual Report."

An amendment to the Amendment in the Nature of a Substitute offered by MR. MEEHAN (#1F); was AGREED TO by voice vote.

Page 14, lines 9 through 21, strike paragraph (3) and insert a new paragraph entitled "(3) Inclusion in Regulatory Regimes."

An amendment to the Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1G); was AGREED TO by voice vote.

Page 17, after line 11, insert a new subsection entitled "(i) Limitation of Regulatory Authority."

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1H); was NOT AGREED TO by voice vote.

Page 24, beginning on line 14, strike section 3 and insert a new section 3 entitled "Sec. 3 Public-Private Clearinghouse."

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1I); was NOT AGREED TO by voice vote.

Page 25, line 8 strike "and developing" and all that follows through "technology" on line 9.

Page 28, line 8, strike "Government;" and all that follows through "; and" on line 22 and insert "Government; and".

Page 33, line 19, strike paragraph (8) and redesignate the subsequent paragraphs accordingly.

An amendment to the Amendment in the Nature of a Substitute offered by MR. KEATING (#1J); was AGREED TO by voice vote.

Page 48, after line 6, insert the following (and renumber the subsequent sections and conform the amendment to the table of contents beginning on page 49, line 17, accordingly):

A new section "Sec. 251. Private Right of Action."

An amendment to the Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1K); was WITHDRAWN by unanimous consent.

Page 52, beginning on line 1, strike section 5 and insert a new section 5 entitled "Sec. 5. Cybersecurity Domestic Preparedness Consortium and Cybersecurity Training Center."

Full Committee Consideration

The Committee met on April 18, 2012, to consider H.R. 3674, and ordered the measure to be reported to the House with a favorable recommendation, amended, by a recorded vote of 16 yeas and 13 nays (Roll Call Vote No. 53). The Committee took the following actions:

The Committee adopted H.R. 3674, as amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. LUNGREN (#1); was AGREED TO by voice vote.

An amendment to the Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1A); was AGREED TO by voice vote.

Page 4, ln 8, insert a new paragraph and renumber: "(c) Acquire, Intercept, Retain, Use, and Disclose Communications and Other System Traffic."

And on Page 7, line 22, insert the following subparagraph and renumber accordingly: "(1) Countermeasures."

And on Page 12 line 23 insert a new section entitled "Sec. 228. Federal Preemption, Exclusivity and Law Enforcement Activities."

An amendment offered by MS. JACKSON LEE to the amendment offered by MR. MCCAUL to the Amendment in the Nature of a Substitute (#1A1); was NOT AGREED TO by voice vote.

At the end of section (c)(1)(D) strike "and"

At the end of section (c)(1)(E), before the period insert: "and the such policies and procedures shall —

"(1) minimize the impact on privacy and civil liberties, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

"(2) reasonably limit the acquisition, interception, retention, use and disclosure of communications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this subtitle, including establishing a process for the timely destruction on recognition of communications, records, system traffic or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related to protecting Federal systems and critical information infrastructure from cybersecurity threats and mitigating cybersecurity threats;

"(3) include requirements to safeguard communications, records, system traffic or other information that can be used to identify specific persons from unauthorized access or acquisition; and

"(4) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific persons to the greatest extent practicable and require recipients of such information to be informed that the communications, records, system traffic or other information disclosed may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the

information is evidence of a crime that has been, is being, or is about to be committed, as specified by the Secretary; and"

Add a section (c)(1)(F) that reads:

"(F) the communications and system traffic to be acquired, intercepted, retained, used or disclosed are transiting to or from or stored on a Federal system."

An amendment to the Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1B); was AGREED TO by voice vote.

Strike section 6 on page 29 and insert a new section 6 entitled "Sec. 6. Cybersecurity Domestic Preparedness Consortium and Cybersecurity Training Center."

An amendment to the Amendment in the Nature of a Substitute offered by MR. KING (#1C); was AGREED TO by voice vote.

Page 13, line 21 after "Department" insert "pursuant to Title XI of the National Security Act of 1947, as amended"

Page 17, line 16 at the end of the sentence insert "consistent with the requirements of Title XI of National Security Act of 1947, as amended"

Page 19, line 23 - after "Government" insert "pursuant to Title XI of National Security Act of 1947, as amended"

Page 20, line 8 after "regulation," insert "including information restricted from disclosure under Title XI of the National Security Act of 1947, as amended"

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON (#1D); was NOT AGREED TO by a recorded vote of 10 yeas and 15 nays (Roll Call Vote No. 39).

Page 10, after line 7, insert a new section entitled "Sec. 226. Identification of Sector Specific Cybersecurity Risks."

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON (#1E); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 40).

Page 10, after line 7, insert a new section entitled "Sec. 226. Identification of Sector Specific Cybersecurity Risks."

An amendment to the Amendment in the Nature of a Substitute offered by MS. SANCHEZ (#1F); was NOT AGREED TO by a recorded vote of 12 yeas and 15 nays (Roll Call Vote No. 41).

Page 17, beginning at line 13, strike the quoted sections 244 through 247 and insert the following new sections entitled "Sec. 244. Annual Report."; "Sec. 245. Advisory Committee."; Sec. 246. Operational Framework."; Sec. 247. Participation."; "Sec. 248. "Advisory Committee Annual Report."; and Sec. 249. Authority to Issue Warnings."

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1G); was NOT AGREED TO by a recorded vote of 12 yeas and 15 nays (Roll Call Vote No. 42).

Page 29, beginning at line 8, strike section 7.

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1H); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 43).

Page 14, beginning at line 4 strike the quotes section 242 and insert a new section entitled "Sec. 142. Establishment of the National Cybersecurity and Communications Integration Center."

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (#1I); was NOT AGREED

TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 44).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Transportation Systems Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MS. RICHARDSON (#1J); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 45).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Chemical Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MS. RICHARDSON (#1K); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 46).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Emergency Services Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MR. KEATING (#1L); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 47).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Nuclear Reactors, Materials, and Waste Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MR. KEATING (#1M); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 48).

Add at the end a new section entitled "Sec. __K. University-Based Regional Research Centers for Cybersecurity."

An amendment to the Amendment in the Nature of a Substitute offered by MR. HIGGINS (#1N); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 49).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Energy Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MR. RICHMOND (#1O); was AGREED TO by voice vote.

Page 14, line 24, strike "Ten" and insert "Eleven".

Page 15, after line 13, insert the following: "(I) Chemical.

An amendment to the Amendment in the Nature of a Substitute offered by MS. HOCHUL (#1P); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 50).

Page 10, line 8, strike "227" and insert "228".

Page 10, beginning line 8, insert a new section entitled "Sec. 227. Identification of Cybersecurity Risks to the Dams Sector."

An amendment to the Amendment in the Nature of a Substitute offered by MS. HAHN (#1Q); was AGREED TO by voice vote.

Page 6, line 19, strike "(f)" and insert "(g)".

Page 6, beginning line 19, insert a new paragraph entitled "(f). Privacy Officer Oversight."

Page 7, line 21, strike "G" and insert "(H)".

An amendment to the Amendment in the Nature of a Substitute offered by MS. HAHN (#1R); was NOT AGREED TO by a recorded vote of 14 yeas and 15 nays (Roll Call Vote No. 51).

Page 2, strike "and" after the semicolon at line 22, and after line 22 insert the following (and redesignate accordingly):

"(6) facilitating the exchange of information among public,. private, and critical infrastructure information networks and the protection of such information by ensuring that all information identifying the submitter and any unnecessary personally identifiable information is deleted from the information exchanged; and.

A Substitute Amendment in the Nature of a Substitute offered by MR. BROUN (#2); was WITHDRAWN by unanimous consent.

A Substitute Amendment in the Nature of a Substitute offered by MR. THOMPSON (#3); was RULED OUT OF ORDER.

A point of order was made by Mr. Lungren that the amendment (#3) was in violation of House Rule XI clause 2(g)(4) and Committee Rule 3 clause 2(a).

The Chair Ruled that the amendment was not in order.

Mr. Thompson appealed the ruling of the Chair

A motion by Mr. Lungren to table the appealing of the ruling of the Chair on the point of order was AGREED TO by a recorded vote of 17 yeas and 11 nays.

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

The Committee on Homeland Security considered H.R. 3674 on April 18, 2012, and took the following recorded votes:

A motion by Mr. Lungren to table the appealing of the ruling of the Chair on the point of order was AGREED TO by a recorded vote of 17 yeas and 11 nays (Roll Call Vote No. 38). The vote was as follows:

YEAS	NAYS
MR. PETER T. KING	MR. BENNIE G. THOMPSON
MR. DANIEL E. LUNGREN	MS. LORETTA SANCHEZ
MR. MIKE ROGERS	MR. HENRY CUELLAR
MR. MICHAEL T. MCCAUL	MS. YVETTE D. CLARKE
MR. GUS M. BILIRAKIS	MS. LAURA RICHARDSON
MR. PAUL C. BROUN	MR. DANNY K. DAVIS
MRS. CANDICE S. MILLER	MR. CEDRIC L. RICHMOND
MR. TIM WALBERG	MR. HANSEN CLARKE
MR. CHIP CRAVAACK	MR. WILLIAM R. KEATING
MR. JOE WALSH	MS. KATHLEEN C. HOCHUL
MR. PATRICK MEEHAN	MS. JANICE HAHN
MR. BENJAMIN QUAYLE	
MR. E. SCOTT RIGELL	
MR. BILLY LONG	
MR. JEFF DUNCAN	
MR. BLAKE FARENTHOLD	
MR. ROBERT L. TURNER	

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON (#1D); was NOT AGREED TO by a re-

corded vote of 10 yeas and 15 nays (Roll Call Vote No. 39). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. SHEILA JACKSON LEE	MR. DANIEL E. LUNGREN
MS. LAURA RICHARDSON	MR. MIKE ROGERS
MR. DANNY K. DAVIS	MR. MICHAEL T. MCCAUL
MR. BRIAN HIGGINS	MR. GUS M. BILIRAKIS
MR. CEDRIC L. RICHMOND	MR. PAUL C. BROUN
MR. HANSEN CLARKE	MRS. CANDICE S. MILLER
MR. WILLIAM R. KEATING	MR. TIM WALBERG
MS. KATHLEEN C. HOCHUL	MR. CHIP CRAVAACK
MS. JANICE HAHN	MR. JOE WALSH
	MR. PATRICK MEEHAN
	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON (#1E); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 40). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. SHEILA JACKSON LEE	MR. DANIEL E. LUNGREN
MR. HENRY CUELLAR	MR. MIKE ROGERS
MS. LAURA RICHARDSON	MR. MICHAEL T. MCCAUL
MR. DANNY K. DAVIS	MR. GUS M. BILIRAKIS
MR. BRIAN HIGGINS	MR. PAUL C. BROUN
MR. CEDRIC L. RICHMOND	MRS. CANDICE S. MILLER
MR. HANSEN CLARKE	MR. TIM WALBERG
MR. WILLIAM R. KEATING	MR. CHIP CRAVAACK
MS. KATHLEEN C. HOCHUL	MR. JOE WALSH
MS. JANICE HAHN	MR. PATRICK MEEHAN
	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. SANCHEZ (#1F); was NOT AGREED TO by a recorded vote of 12 yeas and 15 nays (Roll Call Vote No. 41). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. LAURA RICHARDSON	MR. GUS M. BILIRAKIS
MR. DANNY K. DAVIS	MR. PAUL C. BROUN
MR. BRIAN HIGGINS	MRS. CANDICE S. MILLER
MR. CEDRIC L. RICHMOND	MR. TIM WALBERG
MR. HANSEN CLARKE	MR. CHIP CRAVAACK

MR. WILLIAM R. KEATING	MR. JOE WALSH
MS. KATHLEEN C. HOCHUL	MR. PATRICK MEEHAN
MS. JANICE HAHN	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1G); was NOT AGREED TO by a recorded vote of 12 yeas and 15 nays (Roll Call Vote No. 42). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. LAURA RICHARDSON	MR. GUS M. BILIRAKIS
MR. DANNY K. DAVIS	MR. PAUL C. BROUN
MR. BRIAN HIGGINS	MRS. CANDICE S. MILLER
MR. CEDRIC L. RICHMOND	MR. TIM WALBERG
MR. HANSEN CLARKE	MR. CHIP CRAVAACK
MR. WILLIAM R. KEATING	MR. JOE WALSH
MS. KATHLEEN C. HOCHUL	MR. PATRICK MEEHAN
MS. JANICE HAHN	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. CLARKE (#1H); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 43). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. E. SCOTT RIGELL
MS. JANICE HAHN	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (#1I); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 44). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. E. SCOTT RIGELL
MS. JANICE HAHN	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. RICHARDSON (#1J); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 45). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. E. SCOTT RIGELL
MS. JANICE HAHN	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. RICHARDSON (#1K); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 46). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN

MS. KATHLEEN C. HOCHUL	MR. E. SCOTT RIGELL
MS. JANICE HAHN	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MR. KEATING (#1L); was NOT AGREED TO by a recorded vote of 13 yeas and 15 nays (Roll Call Vote No. 47). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. E. SCOTT RIGELL
MS. JANICE HAHN	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MR. KEATING (#1M); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 48). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. BENJAMIN QUAYLE
MS. JANICE HAHN	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MR. HIGGINS (#1N); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 49). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. BENJAMIN QUAYLE
MS. JANICE HAHN	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. HOCHUL (#1P); was NOT AGREED TO by a recorded vote of 13 yeas and 16 nays (Roll Call Vote No. 50). The vote was as follows:

YEAS	NAYS
MR. BENNIE G. THOMPSON	MR. PETER T. KING
MS. LORETTA SANCHEZ	MR. DANIEL E. LUNGREN
MS. SHEILA JACKSON LEE	MR. MIKE ROGERS
MR. HENRY CUELLAR	MR. MICHAEL T. MCCAUL
MS. YVETTE D. CLARKE	MR. GUS M. BILIRAKIS
MS. LAURA RICHARDSON	MR. PAUL C. BROUN
MR. DANNY K. DAVIS	MRS. CANDICE S. MILLER
MR. BRIAN HIGGINS	MR. TIM WALBERG
MR. CEDRIC L. RICHMOND	MR. CHIP CRAVAACK
MR. HANSEN CLARKE	MR. JOE WALSH
MR. WILLIAM R. KEATING	MR. PATRICK MEEHAN
MS. KATHLEEN C. HOCHUL	MR. BENJAMIN QUAYLE
MS. JANICE HAHN	MR. E. SCOTT RIGELL
	MR. BILLY LONG
	MR. JEFF DUNCAN
	MR. ROBERT L. TURNER

An amendment to the Amendment in the Nature of a Substitute offered by MS. HAHN (#1R); was NOT AGREED TO by a recorded vote of 14 yeas and 15 nays (Roll Call Vote No. 51). The vote was as follows:

YEAS	NAYS
MR. PAUL C. BROUN	MR. PETER T. KING
MR. BENNIE G. THOMPSON	MR. DANIEL E. LUNGREN
MS. LORETTA SANCHEZ	MR. MIKE ROGERS
MS. SHEILA JACKSON LEE	MR. MICHAEL T. MCCAUL
MR. HENRY CUELLAR	MR. GUS M. BILIRAKIS
MS. YVETTE D. CLARKE	MRS. CANDICE S. MILLER
MS. LAURA RICHARDSON	MR. TIM WALBERG
MR. DANNY K. DAVIS	MR. CHIP CRAVAACK
MR. BRIAN HIGGINS	MR. JOE WALSH

Mr. Cedric L. Richmond
Mr. Hansen Clarke
Mr. William R. Keating
Ms. Kathleen C. Hochul
Ms. Janice Hahn
Mr. Patrick Meehan
Mr. Benjamin Quayle
Mr. E. Scott Rigell
Mr. Billy Long
Mr. Jeff Duncan
Mr. Robert L. Turner

The Committee ordered H.R. 3674 to be reported to the House with a favorable recommendation, amended, by a recorded vote of 16 yeas and 13 nays (Roll Call Vote No. 52). The vote was as follows:

YEAS	NAYS
Mr. Peter T. King	Mr. Bennie G. Thompson
Mr. Daniel E. Lungren	Ms. Loretta Sanchez
Mr. Mike Rogers	Ms. Sheila Jackson Lee
Mr. Michael T. McCaul	Mr. Henry Cuellar
Mr. Gus M. Bilirakis	Ms. Yvette D. Clarke
Mr. Paul C. Broun	Ms. Laura Richardson
Mrs. Candice S. Miller	Mr. Danny K. Davis
Mr. Tim Walberg	Mr. Brian Higgins
Mr. Chip Cravaack	Mr. Cedric L. Richmond
Mr. Joe Walsh	Mr. Hansen Clarke
Mr. Patrick Meehan	Mr. William R. Keating
Mr. Benjamin Quayle	Ms. Kathleen C. Hochul
Mr. E. Scott Rigell	Ms. Janice Hahn
Mr. Billy Long	
Mr. Jeff Duncan	
Mr. Robert L. Turner	

Committee Oversight Findings

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

New Budget Authority, Entitlement Authority, and Tax Expenditures

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3674, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011, would result in a new authorization of $4,000,000 for the fiscal years 2013, 2014 and 2015 for the National Cybersecurity and Communications Integration Center.

Congressional Budget Office Estimate

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 20, 2012.

Hon. PETER T. KING,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3674, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2012.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 3674—Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2012

Summary: H.R. 3674 would authorize appropriations for the Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC). The bill also would authorize the Secretary of DHS to establish new programs to provide cybersecurity training for state and local officials. CBO estimates that implementing H.R. 3674 would result in additional discretionary spending totaling $28 million over the next five years, assuming appropriation of the necessary amounts.

Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

H.R. 3674 would impose an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that implementing the mandate would not affect the budgets of state, local, or tribal governments. The bill contains no private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 3674 is shown in the following table. The costs of this legislation fall within budget function 050 (national defense).

	By fiscal year, in millions of dollars—					
	2013	2014	2015	2016	2017	2013–2017
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
National Cybersecurity and Communications Integration Center:						
Authorization Level	4	4	4	0	0	12
Estimated Outlays	3	4	4	1	0	12
Cybersecurity Domestic Preparedness Training for State and Local Authorities:						
Estimated Authorization Level	0	3	5	8	8	24
Estimated Outlays	0	1	3	5	7	16
Total Changes:						
Estimated Authorization Level	4	7	9	8	8	36
Estimated Outlays	3	5	7	6	7	28

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted in late 2012, and that the necessary amounts will be appropriated each year. Under current law, DHS's Office of Cybersecurity and Communications (CS&C) performs most of the ac-

tivities authorized by the bill. CS&C has received appropriations totaling approximately $600 million in fiscal year 2012 to perform those functions on behalf of DHS.

National Cybersecurity and Communications Integration Center

Section 4 would codify the authority for DHS to operate the NCCIC, which was established in October of 2009. The NCCIC is a watch and warning center that monitors threats to the nation's information technology and cyber infrastructure. The bill would authorize $4 million for the NCCIC for fiscal years 2013, 2014, and 2015, slightly less than the $4.5 million received by the center so far in 2012. Assuming appropriation of the authorized amounts, CBO estimates that implementing this provision would cost $12 million over the 2013–2017 period.

Cybersecurity and Domestic Preparedness Training for State and Local Authorities

Section 6 would authorize the Secretary of DHS to establish centers to provide cybersecurity training to state and local first responders and other officials. While DHS has not determined how it would utilize the authorities provided by this provision, CBO expects that such training would be provided at DHS's information and threat-sharing centers (fusion centers). Those centers are used to facilitate information sharing among federal, state, and local authorities. DHS organizes the centers, which are in every state and many metropolitan areas across the country, into nine geographic regions. Assuming that DHS eventually implements such training programs for all nine geographic regions, and that the costs to provide the training are comparable to similar training programs, such as the Cyber Security Education Consortium, CBO estimates that implementing this provision would cost $16 million over the 2013–2017 period, assuming the appropriation of the necessary amounts.

Estimated impact on state, local, and tribal governments: H.R. 3674 would impose an intergovernmental mandate as defined in UMRA because it would preempt state privacy and disclosure laws relating to the interception, acquisition, use, and disclosure of communications and system traffic transmitted to or from federal systems. While that preemption would limit the application of state laws, it would impose no duty on states that would result in additional spending. Therefore, CBO estimates that the mandate would not affect the budgets of state, local, or tribal governments.

Estimated impact on the private sector: The bill contains no new private-sector mandates as defined in UMRA.

Estimate prepared by: Federal Costs: Jason Wheelock; Impact on State, Local, and Tribal Governments: J'nell J. Blanco; Impact on the Private Sector: Elizabeth Bass.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 3674 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

The bill requires the Department of Homeland Security to develop a strategy for its cybersecurity mission. The bill also requires a written charter for the National Cybersecurity and Communications Integration Center (NCCIC). The bill also requires annual reports by the Board of Advisors to the NCCIC. The bill further requires a report on how the Department may help regional, State and local cyber cooperatives.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3674 preempts any State, local or Tribal law regarding the interception, retention, use and disclosure of communications or other system traffic that are transiting to or from or stored on Federal systems for cybersecurity purposes as defined within H.R. 3674.

ADVISORY COMMITTEE STATEMENT

In compliance with section 5(b) of the Federal Advisory Committee Act, requiring the report of any Committee establishing, or authorizing the establishment of any advisory committee to include a statement as to whether the functions of the proposed advisory committee are being or could be performed by one or more agencies or by an advisory committee already in existence, or by enlarging the mandate of an existing advisory committee. The Committee finds:

H.R. 3674 establishes an advisory board to the Secretary of Homeland Security on the efficient operation of the National Cybersecurity and Communications Integration Center in providing timely and actionable information to critical infrastructure owners and operators and other elements of the private sector. This advisory board is composed of members of critical infrastructure and civil liberties and privacy communities. This function could not be performed by another existing advisory board as no existing board has a similar membership. This function could not be performed by another agency as no agency has similar membership for providing both private sector and civil liberty community perspective to the sharing of cyber threat information.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

The bill may be cited as the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011" or, the "PrECISE Act".

Section 2. Department of Homeland Security Cybersecurity Activities.

This section inserts into the Homeland Security Act of 2002, at the end of Subtitle C of title II, new sections.

Section 226 Department of Homeland Security Cybersecurity Activities.

This section provides authority for the Secretary of Homeland Security to perform necessary activities to facilitate the protection of Federal systems and assist private sector critical infrastructure owners and operators in protecting their systems upon request.

This section also authorizes Department of Homeland Security responsibilities regarding information security for the Federal Government. At the direction of the Office of Management and Budget, DHS is authorized to conduct centralized analysis and operate consolidated intrusion prevention technology on behalf of other Federal agencies. In carrying out these activities the Secretary shall coordinate with relevant entities, designate a lead cybersecurity official to coordinate activities within the Department, and develop a strategy that guides the Department's cybersecurity activities.

The Committee does not intend for this legislation to impact any of the Secretary's authorities articulated in Homeland Security Presidential Directive–7 signed December 17, 2003 (HSPD–7). The Committee believes that the Secretary shall continue to operate and perform necessary activities that are consistent with HSPD–7 authorities. These activities would include coordination of national cyber incident response through the drafting and maintenance of a National Cyber Response Plan developed in coordination with the private sector.

The Committee directs the Department to place special emphasis on participation in nationwide outreach and education efforts. The need for improved computer hygiene and for all individuals to take basic steps to better protect themselves and the information for which they are responsible is extremely important. The Department should take every opportunity to educate the public about the importance of cybersecurity, cyber ethics, and ways to promote cybersecurity best practices at home and in the workplace. The Department should support organizations that seek to improve cybersecurity education and the need for improved cybersecurity. The Department should engage whenever possible in popular culture promotions to improve cybersecurity, including public service announcements, and incorporate outreach through popular media outlets.

The Committee believes that the Secretary should make special effort to ensure that the Department is aware of and familiar with the state of the art in cybersecurity technology, and is in a position to incorporate necessary technology to ensure that the Department maintains excellence in its cybersecurity capability. The Secretary should take advantage of the innovation of the private sector, and should ensure that technologies being developed through the Science and Technology Directorate as well as the research, development, testing and evaluation by other government agencies are known and appropriately incorporated into the Department's operations.

Section 227 Personnel Authorities Related to the Office of Cybersecurity and Communication.

This section authorizes the Secretary to designate Federal employees as members of the excepted service, and fix competitive compensation and retention bonuses for these positions.

The Committee believes that the Secretary should be aggressive in exercising these personnel authorities to ensure talented individuals will do the most to improve the quality of the Department's cybersecurity mission. The Secretary should attempt to hire the most qualified and talented employees understanding that talented cybersecurity professionals come with many different, and possibly untraditional, backgrounds and educational experiences.

Section 228 Federal Preemption, Exclusivity and Law Enforcement Activities.

This section provides Federal preemption over other similar State and local statutes regarding the acquisition of information. It also provides another exclusive means to intercept communication under Title 50 and limits the Secretary's law enforcement authority.

Section 2(b) Clerical Amendments.

Section 2(c) Plan for Execution of Authorities.

This section requires the Secretary to submit a report to Congress on how the Department will implement the new authorities granted to it in this section.

The Committee feels this plan for the execution of authorities is critical for providing Congress with a guide for providing oversight of the Department's activities.

Section 3. Department of Homeland Security Information Sharing.

The Homeland Security Act of 2002 is amended by adding the following:

Section 241 Information Sharing.

This section directs the Secretary to ensure that all cyber threat information received in accordance with Section 202 of the Homeland Security Act of 2002 is shared with appropriate critical information infrastructure owners and operators on a timely basis.

The Committee believes this is a crucial section ensuring that critical infrastructure owners and operators have the information necessary to protect their infrastructure, which is one of the most important responsibilities for the Department.

Section 242 Establishment of National Cybersecurity and Communications Integration Center.

This section establishes a center within the Department to facilitate information sharing between the private sector and the Federal Government. The Secretary is directed to share cyber threat information, best practices, support and advice and to properly protect information entrusted to the National Cybersecurity and Communications Integration Center (NCCIC).

The Department should ensure that the NCCIC has facilities that are available to operate at a highly classified level but the Committee believes that the operational floor should be unclassified as much as possible to enable the participation of as many appropriate entities as possible. The Department should implement the National Information Exchange Model to share information with and through the NCCIC. The Committee feels strongly that the Department should incorporate an automated information sharing process in order to speed dissemination of appropriate information. To increase the speed of dissemination the Committee recommends that the Secretary prioritize resources for timely analysis of cyber threat information, to include developing automated processes and procedures for distributing appropriate information within particular communities of interest that are willing to accept a lower level of certainty for increased speed of dissemination.

Section 243 Board of Advisors.

This section establishes a board of advisors to the Secretary on the efficient operation of the National Cybersecurity and Communications Integration Center (NCCIC). The board would be composed of representatives from 14 members of the private sector. Those 14 members would be made up of 11 different critical infrastructure owners and operators, privacy and civil liberty experts, and the chair of the National Council of Information Sharing and Analysis Centers (ISACs). The Board would provide an annual report on the activities of the NCCIC to both the Secretary and Congress.

It is important to note that the Board does not have directive power over the NCCIC, nor can it veto directions of the Secretary, but its recommendations for improving information sharing with the private sector should be given proper weight and consideration. The Secretary should be able to articulate a reason why the Board's recommendations are not implemented.

The Committee expects the Department to provide administrative support to the Board so it can complete its annual report. The Department shall also host the Board's quarterly meetings unless a majority of the Board decides that a meeting in person is not necessary. The Board shall meet in person at least once a year. The Committee does not expect the Department to pay travel expenses of the Board, but it has the authority to do so.

Section 244 Charter.

This section directs the Secretary to develop a charter to govern the operations and administration of the National Cybersecurity and Communications Integration Center (NCCIC) which shall address the following: the organizational structure of the NCCIC; the mission statement of the NCCIC; a plan to promote participation

in the NCCIC; and, procedures for making appropriate information available to outside research groups.

The Committee believes the direction to create a charter provides the Department the opportunity to articulate how it will organize the NCCIC and explain the expectations and responsibilities of all participants involved with the NCCIC. It is important that the charter be made public to ensure that all prospective participants will understand what will be expected of them and what they can expect of other participants. Similarly, the Committee expects the Secretary to articulate through the charter how the Department will protect privacy and civil liberties of United States persons consistent with existing statues, rules and orders. The Department should articulate in the charter what information should be shared with and through the NCCIC, how it will be used and how it will not be used, and what the consequences will be if the information is used contrary to the charter. The Department should use the charter to encourage the sharing of information and to reassure the privacy and civil liberties communities that the Department is not misusing information entrusted to the NCCIC. The Committee expects that the outside groups will only receive information that is stripped of all identifying information of individual entities.

Section 245 Participation.

This section authorizes the Secretary to identify organizations that may participate and collocate with National Cybersecurity and Communications Integration Center (NCCIC).

The Committee feels that the Secretary should encourage participation in the NCCIC by diverse organizations including small, medium and large businesses, State and local governments, and regional cybersecurity organizations. Participation need not be limited to critical infrastructure owners and operators. The Committee believes this provision in addition to the charter obviates any need for a participant of the NCCIC to sign anything other than a simple memorandum of understanding. The agreement between the Department and the prospective participant should demonstrate that both parties are aware of the rules for sharing information and the expectations of the participating organization.

Section 246 Annual Report.

This section requires the National Cybersecurity and Communications Integration Center (NCCIC) board of advisors to submit to the Secretary and appropriate congressional committees an annual report on the status of NCCIC and its performance. Each report shall address the following:

(1) amount of information shared;
(2) number of violations of information sharing procedures;
(3) any changes to Center's charter; and
(4) proposed ways of improving information sharing.

The Committee believes it is important for the Board to create this annual report rather than the Department to maintain an independent voice for the private sector in the NCCIC.

Section 247 Authority to Issue Warnings.

This section allows the Secretary to issue advisories and warnings to any public or private entity or to the general public regarding threats to information networks. The government may not dis-

close the source of the submitted information, or any proprietary or generally private information.

Section 248 Definitions.

This section defines the terms used in the Homeland Security Act of 2002, as amended by H.R. 3674

Section 249 Savings Clause.

This section ensures that nothing in this subtitle limits the authorities of any other Federal agency or impacts existing relationships or authorities of the Department of Homeland Security or other agencies.

Section 3(a)(2) Clerical Amendments.

This section provides for clerical corrections to the Homeland Security Act of 2002 to reflect the changes made within H.R. 3674.

Section 3(b) Authorization of Appropriations for the National Cybersecurity and Communications Integration Center.

This section authorizes $4,000,000 for the National Cybersecurity and Communications Integration Center (NCCIC), which matches the fiscal year 2013 budget request.

Section 4. Cybersecurity Research and Development.

This section requires the Under Secretary for Science and Technology to support research and development designed to protect against acts of terrorism and cyber threats, including work to improve and create technologies for detecting and containing attacks, and preventing future attacks. The Under Secretary shall coordinate activities with the Under Secretary for National Protection and Programs, the Assistant Secretary for Cybersecurity and Communications, and the Assistant Secretary for Infrastructure Protection, the heads of other relevant Federal departments, and foreign partners.

The Committee believes it is important that the operational elements of the cybersecurity mission interact and take advantage of the research and development activities of the Department. Similarly the cybersecurity research and development activities of the Department should complement and support the operational elements.

Section 5. Report on Support for Regional Cybersecurity Cooperatives.

This section requires the Secretary submit to Congress a report on a plan to provide support to regional, State, and local grassroots cybersecurity cooperatives.

Section 6. Cybersecurity Domestic Preparedness Consortium and Cybersecurity Training Center.

This section authorizes the Secretary to establish a consortium of academic, nonprofit and government entities to provide training to State and local first responders, develop curriculum and conduct cybersecurity training and simulation exercises. The section also authorizes a training center and a plan for using fusion centers to train State and local law enforcement personnel.

The Committee authorizes these activities but notes that additional authorization of appropriations was not included in this bill.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

Subtitle C—Information Security

* * * * * * *

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.

* * * * * * *

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, ad-

vice, 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 physical 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.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

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, 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;

(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.

* * * * * * *

COMMITTEE CORRESPONDENCE

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 19, 2012

The Honorable Darrell Issa
Chairman
House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Issa:

On April 18, 2012, the Committee on Homeland Security ordered reported, with amendment, HR 3674, the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011," by a vote of 16-13. The bill was referred primarily to the Committee on Homeland Security, with additional referrals to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence. I have forwarded a copy of the reported text and draft bill report to your Committee staff for review.

I ask that you allow the Committee on the Oversight and Government Reform to be discharged from further consideration of the bill so that it may be scheduled by the Majority Leader. This discharge in no way affects your jurisdiction over the subject matter of the bill, and it will not serve as precedent for future referrals. In addition, should a conference on the bill be necessary, I would support your request to have the Committee on Oversight and Government Reform represented on the conference committee. Finally, I would be pleased to include this letter and any response in the bill report filed by the Committee on Homeland Security to memorialize our understanding.

Sincerely,

PETER T. KING
Chairman

cc: The Honorable John Boehner, Speaker of the House
The Honorable Elijah Cummings
The Honorable Bennie Thompson
Mr. Tom Wickham, House Parliamentarian

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

DAN BURTON, INDIANA
JOHN L. MICA, FLORIDA
TODD RUSSELL PLATTS, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
PATRICK MCHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
CONNIE MACK, FLORIDA
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
ANN MARIE BUERKLE, NEW YORK
PAUL A. GOSAR, D.D.S., ARIZONA
RAUL R. LABRADOR, IDAHO
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DesJARLAIS, M.D., TENNESSEE
JOE WALSH, ILLINOIS
TREY GOWDY, SOUTH CAROLINA
DENNIS A. ROSS, FLORIDA
FRANK C. GUINTA, NEW HAMPSHIRE
BLAKE FARENTHOLD, TEXAS
MIKE KELLY, PENNSYLVANIA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
http://oversight.house.gov

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

EDOLPHUS TOWNS, NEW YORK
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
DENNIS J. KUCINICH, OHIO
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
MIKE QUIGLEY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
BRUCE L. BRALEY, IOWA
PETER WELCH, VERMONT
JOHN A. YARMUTH, KENTUCKY
CHRISTOPHER S. MURPHY, CONNECTICUT
JACKIE SPEIER, CALIFORNIA

April 20, 2012

The Honorable Peter T. King
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On April 18, 2012, the Committee on Homeland Security ordered H.R. 3674, the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011," reported to the House. Thank you for consulting with the Committee on Oversight and Government Reform with regard to H.R. 3674 on those matters within the Committee's jurisdiction. I am writing to confirm our mutual understanding with respect to the consideration of H.R. 3674.

In the interest of expediting the House's consideration of H.R. 3674, I will forego consideration of the bill. However, I do so only with the understanding that this procedural route will not be construed to prejudice the Committee on Oversight and Government Reform's jurisdictional interest and prerogatives on this bill or any other similar legislation and will not be considered as precedent for consideration of matters of jurisdictional interest to my Committee in the future.

Thank you for your commitment to support the appointment of outside conferees from the Committee on Oversight and Government Reform should this bill or a similar bill be considered in a conference with the Senate. I also appreciate you including our exchange of letters on this matter in the Committee Report to accompany H.R. 3674, and in the *Congressional Record* if this bill is considered on the House floor. Thank you for your attention to these matters.

Sincerely,

Darrell Issa
Chairman

Cc: The Honorable John Boehner, Speaker
The Honorable Bennie Thompson
The Honorable Elijah Cummings
Mr. Tom Wickham, Parliamentarian

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 20, 2012

The Honorable Lamar Smith
Chairman
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith:

On April 18, 2012, the Committee on Homeland Security ordered reported, with amendment, HR 3674, the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011," by a vote of 16-13. The bill was referred primarily to the Committee on Homeland Security, with additional referrals to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence. I have forwarded a copy of the reported text and draft bill report to your Committee staff for review.

I ask that you allow the Committee on the Judiciary to be discharged from further consideration of the bill so that it may be scheduled by the Majority Leader. This discharge in no way affects your jurisdiction over the subject matter of the bill, and it will not serve as precedent for future referrals. In addition, should a conference on the bill be necessary, I would support your request to have the Committee on the Judiciary represented on the conference committee. Finally, I would be pleased to include this letter and any response in the bill report filed by the Committee on Homeland Security to memorialize our understanding.

Sincerely,

PETER T. KING
Chairman

cc: The Honorable John Boehner, Speaker of the House
The Honorable Elijah Cummings
The Honorable Bennie Thompson
Mr. Tom Wickham, House Parliamentarian

LAMAR S. SMITH, Texas
CHAIRMAN

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

JOHN CONYERS, JR., Michigan
RANKING MEMBER

HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
(Vacancy)

April 23, 2012

HAND-DELIVERED

The Honorable Peter T. King
Chairman
Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman King,

On April 18, 2012, the Committee on Homeland Security ordered H.R. 3674, the "PRECISE Act of 2011," as amended, to be reported favorably to the House. As a result of your having consulted with the Judiciary Committee concerning provisions of the bill that fall within our Rule X jurisdiction, I am able to agree to discharging our committee from further consideration of the bill so that the bill may proceed expeditiously to the House Floor.

The Judiciary Committee takes this action with our mutual understanding that, by foregoing consideration of H.R. 3674 at this time, we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and that our committee will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues that fall within our Rule X jurisdiction. Our committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and I appreciate your support for any this request.

Finally, I appreciate your April 20 letter confirming this understanding with respect to H.R. 3674, and ask that a copy of our exchange of letters on this matter be included in your committee's report on H.R. 3674 and/or in the *Congressional Record* during floor consideration thereof.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable John Boehner
The Honorable John Conyers, Jr.
The Honorable Bennie G. Thompson
Mr. Tom Wickham, Parliamentarian

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 20, 2012

The Honorable Mike Rogers
Chairman
House Permanent Select Committee Intelligence
HVC-304
Washington, DC 20515

Dear Chairman Rogers:

On April 18, 2012, the Committee on Homeland Security ordered reported, with amendment, HR 3674, the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011," by a vote of 16-13. The bill was referred primarily to the Committee on Homeland Security, with additional referrals to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence. I have forwarded a copy of the reported text and draft bill report to your Committee staff for review. Based on discussions with your staff, I added language to the bill to ensure that the authorization of sections 241, 244, and 247 be limited pursuant to Title XI of the National Security Act, as amended, in accordance with the language included in H.R. 3523, the Cyber Intelligence Security Protection Act. As we move forward, I will continue to work with you to ensure that the language is clarified to more closely align with section 1104(b) as added by H.R. 3523.

I ask that you allow the Permanent Select Committee on Intelligence to be discharged from further consideration of the bill so that it may be scheduled by the Majority Leader. This discharge in no way affects your jurisdiction over the subject matter of the bill, and it will not serve as precedent for future referrals. In addition, should a conference on the bill be necessary, I would support your request to have the Permanent Select Committee on Intelligence represented on the conference committee. Finally, I would be pleased to include this letter and any response in the bill report filed by the Committee on Homeland Security to memorialize our understanding.

Sincerely,

PETER T. KING
Chairman

Mike Rogers, Michigan, CHAIRMAN
Mac Thornberry, Texas
Sue Myrick, North Carolina
Jeff Miller, Florida
K. Michael Conaway, Texas
Peter T. King, New York
Frank A. LoBiondo, New Jersey
Devin Nunes, California
Lynn A. Westmoreland, Georgia
Michele Bachmann, Minnesota
Thomas J. Rooney, Florida
Joseph J. Heck, Nevada

C.A. Dutch Ruppersberger, Maryland, RANKING MEMBER
Mike Thompson, California
Janice D. Schakowsky, Illinois
James R. Langevin, Rhode Island
Adam B. Schiff, California
Dan Boren, Oklahoma
Luis V. Gutierrez, Illinois
Ben Chandler, Kentucky

John A. Boehner, SPEAKER OF THE HOUSE
Nancy Pelosi, DEMOCRATIC LEADER

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

HVC-304, THE CAPITOL
WASHINGTON, DC 20515
(202) 225-4121

Michael Allen, STAFF DIRECTOR

April 23, 2012

The Honorable Peter King
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

In recognition of the importance of expediting the passage of H.R. 3674, the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011," the Permanent Select Committee on Intelligence hereby waives further consideration of the bill. The Committee has jurisdictional interests in H.R. 3674, including intelligence and intelligence-related authorizations and provisions contained in the bill.

We very much appreciate the efforts of you and your staff to address issues of jurisdictional interest to the Permanent Select Committee on Intelligence during consideration of this legislation by the Committee on Homeland Security.

The Committee takes this action only with the understanding that this procedural route should not be construed to prejudice the House Permanent Select Committee on Intelligence's jurisdictional interest over this bill or any similar bill and will not be considered as precedent for consideration of matters of jurisdictional interest to the Committee in the future, including in connection with any subsequent consideration of the bill by the House. In addition, the Permanent Select Committee on Intelligence will seek conferees on any provisions of the bill that are within its jurisdiction during any House-Senate conference that may be convened on this legislation.

Finally, I would ask that you include a copy of our exchange of letters on this matter in the Congressional Record during the House debate on H.R. 3674. I appreciate the constructive work between our committees on this matter and thank you for your consideration.

Sincerely,

Mike Rogers
Chairman

cc: The Honorable John Boehner, Speaker of the House
The Honorable Dutch Ruppersberger, Ranking Member
Mr. Tom Wickham, Parliamentarian

DISSENTING VIEWS

Committee Democrats believe that while H.R. 3674, as favorably forwarded by the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies in February was not perfect, it took a number of steps in the right direction to bolster the Nation's cybersecurity efforts, particularly with respect to helping critical infrastructure owners and operators mitigate risks to their networks. Regrettably, in the intervening months, that balanced, bipartisan bill was replaced, apparently at the insistence of House Republican Leadership, with a shell bill that, in large part, fails to meaningfully address a foremost homeland security concern of current and former national security officials—our Nation's vulnerability to cyber attacks.

During the markup, we expressed our particular concern with the bill's failure to foster greater network security for critical infrastructure. Numerous current and former top national security officials, the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, the Obama Administration's cybersecurity legislative proposal, and even the House Republican's cybersecurity task force recognized the need for action to address systemic vulnerabilities in critical infrastructure networks. Yet, the Majority rejected not only a comprehensive critical infrastructure amendment offered by Ranking Member Thompson but also targeted amendments to provide "best practices" for network security to operators in the Nuclear, Energy, Emergency Services, Chemical, Transportation, and Dams sectors. We would note that the February version of H.R. 3674, as approved on a bipartisan basis, included similar language but the Majority, apparently under pressure from House Republican Leadership, stripped out all language that would address critical infrastructure vulnerabilities—not only regulatory language, but language empowering critical infrastructure owners and operators to make their systems more secure.

We are also troubled that H.R. 3674, as considered at the Full Committee, calls into question the future Federal role of the Department of Homeland Security (DHS) with respect to cybersecurity. Since 2003, pursuant to Homeland Security Presidential Directive–7, DHS has been the "focal point for the security of cyberspace" and in that capacity, has been responsible for (1) providing "analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems" and (2) protecting Federal civilian networks. As approved, the bill encourages inefficiency and duplication of efforts from other departments and agencies by leaving ambiguous lines of authority in the Federal government's cybersecurity posture. This approach is worrisome and reminiscent of a pre-September 11th, 2001 environment, where amidst the chronic

turf wars and stovepiping of the Intelligence Community, there was no lead agency to marshal all the resources at the government's disposal to prevent a catastrophe.

Congressional Committees are incubators of expertise, where groups of Members come together to conduct oversight, develop specialized knowledge on complex issues, and translate that knowledge into legislation for presentation to the Full House. In this case, it appears that the House Republican Leadership supplanted the bipartisan policy priorities of this Committee with its own priorities and, as a result, a measured, thoughtful and targeted bill was swapped for an inadequate measure.

BENNIE G. THOMPSON.
SHEILA JACKSON LEE.
YVETTE D. CLARKE.
DANNY K. DAVIS.
CEDRIC L. RICHMOND.
WILLIAM R. KEATING.
JANICE HAHN.
LORETTA SANCHEZ.
HENRY CUELLAR.
LAURA RICHARDSON.
BRIAN HIGGINS.
HANSEN CLARKE.
KATHLEEN C. HOCHUL.

○