AMENDMENT TO THE RULES COMMITTEE PRINT OF H.R. 3523

OFFERED BY MR. THOMPSON OF MISSISSIPPI

Page 1, strike line 1 and insert the following:

TITLE I—CYBER INTELLIGENCE SHARING AND PROTECTION ACT

SEC. 101. SHORT TITLE.

Page 1, line 2, strike ''Act'' and insert ''title''.

Page 1, line 4, strike ''**2.**'' and insert ''**102.**''

Page 17, line 20, strike ''Act'' and insert ''title''.

Page 18, line 20, strike ''Act'' and insert ''title''.

At the end of the bill, add the following new title:

TITLE II—PROMOTING AND ENHANCING CYBERSECURITY AND INFORMATION SHARING EFFECTIVENESS ACT OF 2012

SEC. 201. SHORT TITLE.

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

SEC. 202. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY ACTIVITIES.

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

"SEC. 226. NATIONAL CYBERSECURITY AUTHORITY.

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

''(1) develop and conduct risk assessments for Federal systems and, subject to the availability of resources and upon request from critical infrastructure owners and operators, critical infrastructure information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing, or other comprehensive assessments techniques;

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

prehensive protective capabilities and other technological solutions;

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

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

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

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

''(C) facilitating information sharing, interactions, and collaborations among and between Federal agencies, State and local governments,

the private sector, academia, and international partners;

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

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

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

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

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

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

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

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

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

''(C) training opportunities to support the development of an effective national cybersecu-

rity workforce and educational paths to cybersecurity professions;

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

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

''(9) develop and conduct exercises, simulations, and other activities designed to support the national response to terrorism and other cybersecurity

threats and incidents and evaluate the national cyber incident response plan and supporting plans developed in accordance with paragraph (8);

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

''(11) subject to the availability of resources, provide technical assistance, including sending on-site teams, to critical infrastructure owners and operators when requested; and

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

''(b) COORDINATION.—

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

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

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

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

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

''(E) academia; and

''(F) international organizations and foreign partners.

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

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

''(4) REPORTS TO CONGRESS.—The lead cybersecurity official shall make annual reports to the ap-

propriate committees of Congress on the coordination of cyber-related programs across the Department.

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

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

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

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

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

''(d) NO RIGHT OR BENEFIT.—The provision of assistance or information to governmental or private entities that own or operate critical infrastructure information systems under this section shall be at the discretion of the Secretary and subject to the availability of resources. The provision of certain assistance or information to one gov-

ernmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

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

''(f) DEFINITIONS.—In this section:

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

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

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

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

essary to ensure essential government operations continue.

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

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

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

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

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

''(3) The owners and operators of critical infrastructure, including as a priority, the relevant Crit-

ical Infrastructure Partnership Advisory Council entities.

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

''(b) EVALUATION OF RISKS.—The Secretary, in coordination with the individuals and entities referred to in subsection (a), shall evaluate the cybersecurity risks identified under subsection (a) by taking into account each of the following:

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

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

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

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

''(5) Other risk-based security factors that the Secretary, in consultation with the head of the sec-

tor specific agency with responsibility for critical infrastructure and the head of any Federal agency that is not a sector specific agency with responsibilities for regulating critical infrastructure, and in consultation with any private sector entity determined appropriate by the Secretary to protect public health and safety, critical infrastructure, or national and economic security.

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

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

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

the typical implementation of each performance standard, of each of the following:

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

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

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

''(3) INCLUSION IN REGULATORY REGIMES.—The heads of sector specific agencies with responsibility for regulating covered critical infrastructure or the head of any Federal agency that is not a sector specific agency with responsibilities for regulating covered critical infrastructure, in consultation with the Secretary and with any private sector entity determined appropriate by the Secretary, shall—

''(A) review agency regulations regarding critical infrastructure protection to determine the efficacy of such regulations in regard to the risks identified under subsection (a);

''(B) revoke any unnecessary or duplicative regulation;

''(C) identify any gaps in regulation that leave any risk to the agency's sector identified under subsection (a) unmitigated;

''(D) propose through a notice and comment rulemaking to include only the most effective and cost beneficial standards collected under paragraph (1) to mitigate unmitigated risks; and

''(E) communicate to covered critical infrastructure the results and basis of the review of regulatory requirements.

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

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

''(2) engage with the National Institute of Standards and Technology and appropriate inter-

national consensus bodies that develop and strengthen standards and practices to address the identified risk.

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

''(1) a significant loss of life;

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

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

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

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

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

''(g) WRITTEN NOTIFICATION.—The Secretary shall provide written notification to the owners or operators of

a facility or function that has been designated a covered critical infrastructure within 30 days of such designation.

''(h) REDRESS.—

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

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

''(3) COMPLIANCE.—The owner or operator of a facility or function identified as covered critical infrastructure shall comply with any requirement of this subtitle relating to covered critical infrastructure until such time as the facility or function is no longer identified as covered critical infrastructure, based on—

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

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

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

''(i) LIMITATION OF REGULATORY AUTHORITY.—Nothing in this section expands the regulatory authority of sector specific agencies or other agencies with regulatory authority over elements of covered critical infrastructure beyond the risk-based performance standards collected under subsection (d).

''SEC. 228. INFORMATION SHARING.

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

''(b) INFORMATION SHARING.—The Secretary shall, in a timely manner and to the maximum extent possible, consistent with rules for the handling of classified and sensitive but unclassified information, share relevant information regarding cybersecurity threats and vulnerabilities, and any proposed actions to mitigate them, with all Federal agencies, appropriate State or local government representatives, appropriate critical infrastructure informa-

tion systems owners and operators, Information Sharing and Analysis Centers, appropriate academic and private sector entitles that conduct cybersecurity or information security research and development, and appropriate private sector entities that provide cybersecurity or information security products or services, including by expediting necessary security clearances for designated points of contact for all appropriate entities.

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

''SEC. 229. CYBERSECURITY RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—The Under Secretary for Science and Technology shall support research, development, testing, evaluation, and transition of cybersecurity technology

in coordination with a national cybersecurity research and development plan. Such support shall include 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 technologies are 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 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 work-

ing groups established by the President to identify unmet needs and cooperatively support activities, as appropriate.

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

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

"(b) COMPENSATION.—The Secretary may—

"(1) fix the compensation of individuals who serve in positions referred to in subsection (a) in relation to the rates of pay provided for comparable positions in the Department and subject to the same limitations on maximum rates of pay established for

employees of the Department by law or regulations; and

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

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

''(d) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a detailed report that includes, for the period covered by the report—

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

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

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

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

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

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

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

''(3) long-term and short-term strategic goals to address critical skills deficiencies, including an analysis of the numbers of and reasons for attrition of employees and barriers to recruiting and hiring individuals qualified in cybersecurity.''.

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

''Sec. 226. National cybersecurity authority.

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

SEC. 203. REPORT ON SUPPORT FOR REGIONAL CYBERSECURITY COOPERATIVES.

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

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

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

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

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

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

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

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

SEC. 204. PILOT PROGRAM ON CYBERSECURITY TRAINING FOR FUSION CENTERS.

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

(b) PILOT PROGRAM.—

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

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

SEC. 205. ASSESSMENT OF SECTOR BY SECTOR CYBERSECURITY PREPAREDNESS.

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

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

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

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

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

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

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

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

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

SEC. 206. REPORT ON FOREIGN ENTITIES POSING CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE.

The Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives a report on the foreign entities, including foreign terrorist organizations, that the Secretary determines pose the greatest cybersecurity threats to the critical infrastructure of the United States.

☒