I

113TH CONGRESS
1ST SESSION

H. R. 3696

To amend the Homeland Security Act of 2002 to make certain improvements regarding cybersecurity and critical infrastructure protection, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 11, 2013

Mr. MCCAUL (for himself, Mr. MEEHAN, Mr. THOMPSON of Mississippi, and Ms. CLARKE) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Science, Space, and Technology and Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend the Homeland Security Act of 2002 to make certain improvements regarding cybersecurity and critical infrastructure protection, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

SEC. 101. HOMELAND SECURITY ACT OF 2002 DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following new paragraphs:

''(19) The term 'critical infrastructure' has the meaning given that term in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e)).

''(20) The term 'critical infrastructure owner' means a person that owns critical infrastructure.

''(21) The term 'critical infrastructure operator' means a critical infrastructure owner or other person that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure.

''(22) The term 'cyber incident' means an incident resulting in, or an attempt to cause an incident that, if successful, would—

''(A) jeopardize or imminently jeopardize, without lawful authority, the security, integrity, confidentiality, or availability of an information system or network of information systems or any information stored on, processed on, or transiting such a system;

''(B) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies related to an information system or network of information systems, or an act of terrorism against an information system or network of information systems; or

''(C) result in the denial of access to or degradation, disruption, or destruction of an information system or network of information systems, or the defeat of an operations control or technical control essential to the security or operation of an information system or network of information systems.

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

''(24) The term 'cybersecurity purpose' means the purpose of ensuring the security, integrity, confidentiality, or availability of, or safeguarding, an information system or network of information systems, including protecting an information system or network of information systems, or data residing on an information system or network of information systems, including protection of an information system or network of information systems, from—

''(A) a vulnerability of an information system or network of information systems;

''(B) a threat to the security, integrity, confidentiality, or availability of an information system or network of information systems, or any information stored on, processed on, or transiting such a system or network;

''(C) efforts to deny access to or degrade, disrupt, or destroy an information system or network of information systems; or

''(D) efforts to gain unauthorized access to an information system or network of information systems, including to gain such unauthor-

ized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network.

''(25) The term 'cybersecurity system' means a system designed or employed to ensure the security, integrity, confidentiality, or availability of, or safeguard, an information system or network of information systems, including protecting such a system or network from—

''(A) a vulnerability of an information system or network of information systems;

''(B) a threat to the security, integrity, confidentiality, or availability of an information system or network of information systems or any information stored on, processed on, or transiting such a system or network;

''(C) efforts to deny access to or degrade, disrupt, or destroy an information system or network of information systems of a private entity; or

''(D) efforts to gain unauthorized access to an information system or network of information systems, including to gain such unauthorized access for the purpose of exfiltrating infor-

mation stored on, processed on, or transiting such a system or network.

''(26) The term 'cyber threat' means any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the security, integrity, confidentiality, or availability of an information system or network of information systems, or information that is stored on, processed by, or transiting an information system or network of information systems.

''(27) The term 'cyber threat information' means information directly pertaining to—

''(A) a vulnerability of an information system or network of information systems of a government or private entity;

''(B) a threat to the security, integrity, confidentiality, or availability of an information system or network of information systems of a government or private entity or any information stored on, processed on, or transiting such a system or network;

''(C) efforts to deny access to or degrade, disrupt, or destroy an information system or network of information systems of a government or private entity;

''(D) efforts to gain unauthorized access to an information system or network of information systems of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network; or

''(E) an act of terrorism against an information system or network of information systems.

''(28) The term 'Federal civilian information systems'—

''(A) means information, information systems, and networks of information systems that are owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including information systems or networks of information systems used or operated by another entity on behalf of a Federal agency; but

''(B) does not include—

''(i) a national security system; or

''(ii) information, information systems, and networks of information systems that are owned, operated, controlled, or licensed solely for use by, or on behalf of,

the Department of Defense, a military department, or an element of the intelligence community.

''(29) The term 'information security' means the protection of information, information systems, and networks of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, including guarding against improper information modification or destruction, including ensuring nonrepudiation and authenticity;

''(B) confidentiality, including preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, including ensuring timely and reliable access to and use of information.

''(30) The term 'information system' means the underlying framework and functions used to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

''(31) The term 'private entity' means any individual or any private or publically-traded company, public or private utility, organization, or corporation, including an officer, employee, or agent thereof.

''(32) The term 'protected private entity' means an entity, other than an individual, that enters into a contract with a cybersecurity provider for goods and services to be used for cybersecurity purposes.

''(33) The term 'shared situational awareness' means an environment in which cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.''.

SEC. 102. ENHANCEMENT OF CYBERSECURITY.

(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 section:

''SEC. 226. ENHANCEMENT OF CYBERSECURITY.

''The Secretary, in collaboration with the heads of other appropriate Federal Government entities, shall conduct activities for cybersecurity purposes, including the provision of shared situational awareness to each other to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.''.

(b) CLERICAL AMENDMENTS.—

(1) SUBTITLE HEADING.—The heading for subtitle C of title II of such Act is amended to read as follows:

"Subtitle C—Cybersecurity and Information Sharing".

(2) TABLE OF CONTENTS.—The table of contents in section 1(b) of such Act is amended—

(A) by adding after the item relating to section 225 the following new item:

"Sec. 226. Enhancement of cybersecurity.";

and

(B) by striking the item relating to subtitle C of title II and inserting the following new item:

"Subtitle C—Cybersecurity and Information Sharing".

SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 102, is further amended by adding at the end the following new section:

"SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

"(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

''(1) IN GENERAL.—The Secretary shall coordinate, on an ongoing basis, with Federal, State, and local governments, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to—

''(A) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

''(B) ensure that Department policies and procedures enable critical infrastructure owners and critical infrastructure operators to receive real-time, actionable, and relevant cyber threat information;

''(C) seek industry sector-specific expertise to—

''(i) assist in the development of voluntary security and resiliency strategies; and

''(ii) ensure that the allocation of Federal resources are cost effective and reduce any burden on critical infrastructure owners and critical infrastructure operators;

''(D) upon request, facilitate and assist risk management efforts of entities to reduce

vulnerabilities, identify and disrupt threats, and minimize consequences to their critical infrastructure;

"(E) upon request, provide education and assistance to critical infrastructure owners and critical infrastructure operators on how they may use protective measures and countermeasures to strengthen the security and resilience of the Nation's critical infrastructure; and

"(F) coordinate a research and development strategy to facilitate and promote advancements and innovation in cybersecurity technologies to protect critical infrastructure.

"(2) ADDITIONAL RESPONSIBILITIES.—The Secretary shall—

"(A) manage Federal efforts to secure, protect, and ensure the resiliency of Federal civilian information systems, and, upon request, support critical infrastructure owners' and critical infrastructure operators' efforts to secure, protect, and ensure the resiliency of critical infrastructure from cyber threats;

"(B) direct an entity within the Department to serve as a Federal civilian entity by and among Federal, State, and local govern-

ments, private entities, and critical infrastructure sectors to provide multi-directional sharing of real-time, actionable, and relevant cyber threat information;

''(C) promote a national awareness effort to educate the general public on the importance of securing information systems;

''(D) upon request, facilitate expeditious cyber incident response and recovery assistance, and provide analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis and consequence management support, and other remote or on-site technical assistance with the heads of other appropriate Federal agencies to Federal, State, and local government entities and private entities for cyber incidents affecting critical infrastructure; and

''(E) engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States upon which the United States depends.

''(3) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require any private

entity to request assistance from the Secretary, or require any private entity requesting such assistance to implement any measure or recommendation suggested by the Secretary.

''(b) CRITICAL INFRASTRUCTURE SECTORS.—The Secretary, in collaboration with the heads of other appropriate Federal agencies, shall designate critical infrastructure sectors (that may include subdivisions of sectors within a sector as the Secretary may determine appropriate). The critical infrastructure sectors designated under this subsection may include the following:

''(1) Chemical.

''(2) Commercial facilities.

''(3) Communications.

''(4) Critical manufacturing.

''(5) Dams.

''(6) Defense Industrial Base.

''(7) Emergency services.

''(8) Energy.

''(9) Financial services.

''(10) Food and agriculture.

''(11) Government facilities.

''(12) Healthcare and public health.

''(13) Information technology.

''(14) Nuclear reactors, materials, and waste.

''(15) Transportation systems.

''(16) Water and wastewater systems.

''(17) Such other sectors as the Secretary determines appropriate.

''(c) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of November 1, 2013, as the 'Sector Specific Agency' for each critical infrastructure sector designated under subsection (b). If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for the purposes of this section, the Secretary shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency shall—

''(1) support the security and resilience activities of the relevant critical infrastructure sector in accordance with this subtitle; and

''(2) provide institutional knowledge and specialized expertise to the relevant critical infrastructure sector.

''(d) SECTOR COORDINATING COUNCILS.—

''(1) RECOGNITION.—The Secretary, in collaboration with each critical infrastructure sector and the relevant Sector Specific Agency, shall recognize

the Sector Coordinating Council for each critical infrastructure sector designated under subsection (b) to coordinate with each such sector on security and resilience activities and emergency response and recovery efforts.

''(2) MEMBERSHIP.—

''(A) IN GENERAL.—The Sector Coordinating Council for a critical infrastructure sector designated under subsection (b) shall—

''(i) be comprised exclusively of relevant critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector;

''(ii) reflect the unique composition of each sector; and

''(iii) include relevant small, medium, and large critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector.

''(B) PROHIBITION.—No government entity with regulating authority shall be a member of the Sector Coordinating Council.

''(3) ROLES AND RESPONSIBILITIES.—The Sector Coordinating Council for a critical infrastructure sector shall—

''(A) serve as a self-governing, self-organized primary policy, planning, and strategic communications entity for coordinating with the Department, the relevant Sector-Specific Agency designated under subsection (c), and the relevant Information Sharing and Analysis Centers under subsection (e) on security and resilience activities and emergency response and recovery efforts;

''(B) establish governance and operating procedures, and designate a chairperson for the sector to carry out the activities described in this subsection;

''(C) coordinate with the Department, the relevant Information Sharing and Analysis Centers under subsection (e), and other Sector Coordinating Councils to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

''(D) provide any recommendations to the Department on infrastructure protection tech-

nology gaps to help inform research and development efforts at the Department.

''(e) SECTOR INFORMATION SHARING AND ANALYSIS CENTERS.—

''(1) RECOGNITION.—The Secretary, in collaboration with the relevant Sector Coordinating Council and the critical infrastructure sector represented by such Council, and in coordination with the relevant Sector Specific Agency, shall recognize at least one Information Sharing and Analysis Center for each critical infrastructure sector designated under subsection (b) for purposes of paragraph (3). No other Information Sharing and Analysis Organizations, including Information Sharing and Analysis Centers, may be precluded from having an information sharing relationship within the National Cybersecurity and Communications Integration Center established pursuant to section 228. Nothing in this subsection or any other provision of this subtitle may be construed to limit, restrict, or condition any private entity or activity utilized by, among, or between private entities.

''(2) ROLES AND RESPONSIBILITIES.—In addition to such other activities as may be authorized by

law, at least one Information Sharing and Analysis Center for a critical infrastructure sector shall—

"(A) serve as an information sharing resource for such sector and promote ongoing multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among such sector, the Department, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers;

"(B) establish governance and operating procedures to carry out the activities conducted under this subsection;

"(C) serve as an emergency response and recovery operations coordination point for such sector, and upon request, facilitate cyber incident response capabilities in coordination with the Department, the relevant Sector Specific Agency and the relevant Sector Coordinating Council;

"(D) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

''(E) coordinate with the Department, the relevant Sector Coordinating Council, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers on the development, integration, and implementation of procedures to support technology neutral, real-time information sharing capabilities and mechanisms within the National Cybersecurity and Communications Integration Center established pursuant to section 228, including—

''(i) the establishment of a mechanism to voluntarily report identified vulnerabilities and opportunities for improvement;

''(ii) the establishment of metrics to assess the effectiveness and timeliness of the Department's and Information Sharing and Analysis Centers' information sharing capabilities; and

''(iii) the establishment of a mechanism for anonymous suggestions and comments;

''(F) implement an integration and analysis function to inform sector planning, risk mitigation, and operational activities regarding

the protection of each critical infrastructure sector from cyber incidents;

''(G) combine consequence, vulnerability, and threat information to share actionable assessments of critical infrastructure sector risks from cyber incidents;

''(H) coordinate with the Department, the relevant Sector Specific Agency, and the relevant Sector Coordinating Council to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

''(I) safeguard cyber threat information from unauthorized disclosure.

''(3) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Cybersecurity and Communications Office of the Department, the Secretary is authorized to use not less than $25,000,000 for any such year for operations support at the National Cybersecurity and Communications Integration Center established under section 228(a) of all recognized Information Sharing and Analysis Centers under paragraph (1) of this subsection.

''(f) CLEARANCES.—The Secretary shall expedite the processing of security clearances under Executive Order 13549 or successor orders to appropriate members of the Sector Coordinating Councils and the critical infrastructure sector Information Sharing and Analysis Centers.

''(g) PUBLIC-PRIVATE COLLABORATION.—The Secretary, in collaboration with the critical infrastructure sectors designated under subsection (b), such sectors' Sector Specific Agencies recognized under subsection (c), and the Sector Coordinating Councils recognized under subsection (d), shall—

''(1) conduct an analysis and review of the existing public-private partnership model and evaluate how the model between the Department and critical infrastructure owners and critical infrastructure operators can be improved to ensure the Department, critical infrastructure owners, and critical infrastructure operators are equal partners and regularly collaborate on all programs and activities of the Department to protect critical infrastructure;

''(2) develop procedures to ensure continuous, collaborative, and effective interactions between the Department, critical infrastructure owners, and critical infrastructure operators; and

''(3) ensure critical infrastructure sectors have a reasonable period for review and comment of all jointly produced materials with the Department.

''(h) PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.—

''(1) IN GENERAL.—The Secretary shall administer the operational information security activities and functions to protect and ensure the resiliency of all Federal civilian information systems.

''(2) ROLES AND RESPONSIBILITIES.—The Secretary, in coordination with the heads of other Federal civilian agencies, shall—

''(A) develop, issue, and oversee the implementation and compliance of all operational information security policies and procedures to protect and ensure the resiliency of Federal civilian information systems;

''(B) administer Federal Government-wide efforts to develop and provide adequate, risk-based, cost-effective, and technology neutral information security capabilities;

''(C) establish and sustain continuous diagnostics systems for Federal civilian information systems to aggregate data and identify

and prioritize the mitigation of cyber vulnerabilities in such systems for cybersecurity purposes;

''(D) develop, acquire, and operate an integrated and consolidated system of intrusion detection, analytics, intrusion prevention, and other information sharing and protective capabilities to defend Federal civilian information systems from cyber threats;

''(E) develop and conduct targeted risk assessments and operational evaluations of Federal civilian information systems, in consultation with government and private entities that own and operate such information systems, including threat, vulnerability, and impact assessments and penetration testing;

''(F) develop and provide technical assistance and cyber incident response capabilities to secure and ensure the resilience of Federal civilian information systems;

''(G) review annually the operational information security activities and functions of each of the Federal civilian agencies;

''(H) develop minimum technology neutral operational requirements for network and secu-

rity operations centers to facilitate the protection of all Federal civilian information systems;

"(I) develop reporting requirements, consistent with relevant law, to ensure the National Cybersecurity and Communications Integration Center established pursuant to section 228 receives all actionable cyber threat information identified on Federal civilian information systems;

"(J) develop technology neutral performance requirements and metrics for the security of Federal civilian information systems;

"(K) implement training requirements that include industry recognized certifications to ensure that Federal civilian agencies are able to fully and timely comply with policies and procedures issued by the Secretary under this subsection; and

"(L) develop training requirements regarding privacy, civil rights, civil liberties, and information oversight for information security employees who operate Federal civilian information systems.

"(3) USE OF CERTAIN COMMUNICATIONS.—

"(A) IN GENERAL.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain, in accordance with applicable law, the assistance of private entities that provide electronic communication services, remote computing services, or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic, deploy countermeasures, or otherwise operate protective capabilities in accordance with subparagraphs (C), (D), (E), and (F) of paragraph (2). No cause of action shall exist against private entities for assistance provided to the Secretary in accordance with this subsection.

"(B) RULE OF CONSTRUCTION.—Nothing in subparagraph (A) may be construed to—

"(i) require or compel any private entity to enter in a contract or agreement described in such subparagraph; or

"(ii) authorize the Secretary to take any action with respect to any communications or system traffic transiting or residing on any information system or network

of information systems other than a Federal civilian information system.

''(i) RULE OF CONSTRUCTION.—No provision of this title may be construed as modifying, limiting, or otherwise affecting the authority of any other Federal agency under any other provision of law.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to such subtitle the following new item:

''Sec. 227. Protection of critical infrastructure and information sharing.''.

SEC. 104. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102 and 103, is further amended by adding at the end the following new section:

''SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

''(a) ESTABLISHMENT.—There is established in the Department the National Cybersecurity and Communications Integration Center (referred to in this section as the 'Center'), which shall be a Federal civilian information sharing interface that provides shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government, and share cyber

threat information by and among Federal, State, and local government entities, Information Sharing and Analysis Centers, private entities, and critical infrastructure owners and critical infrastructure operators that have an information sharing relationship with the Center.

''(b) COMPOSITION.—The Center shall include each of the following entities:

''(1) At least one Information Sharing and Analysis Center established under section 227(e) for each critical infrastructure sector.

''(2) The Multi-State Information Sharing and Analysis Center to collaborate with State and local governments.

''(3) The United States Computer Emergency Readiness Team to coordinate cyber threat information sharing, proactively manage cyber risks to the United States, collaboratively respond to cyber incidents, provide technical assistance to information system owners and operators, and disseminate timely notifications regarding current and potential cyber threats and vulnerabilities.

''(4) The Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators and

share industrial control systems-related security incidents and mitigation measures.

''(5) The National Coordinating Center for Telecommunications to coordinate the protection, response, and recovery of national security emergency communications.

''(6) Such other Federal, State, and local government entities, private entities, organizations, or individuals as the Secretary may consider appropriate that agree to be included.

''(c) CYBER INCIDENT.—In the event of a cyber incident, the Secretary may grant the entities referred to in subsection (a) immediate temporary access to the Center as a situation may warrant.

''(d) ROLES AND RESPONSIBILITIES.—The Center shall—

''(1) promote ongoing multi-directional sharing by and among the entities referred to in subsection (a) of timely and actionable cyber threat information and analysis on a real-time basis that includes emerging trends, evolving threats, incident reports, intelligence information, risk assessments, and best practices;

''(2) coordinate with other Federal agencies to streamline and reduce redundant reporting of cyber threat information;

''(3) provide, upon request, timely technical assistance and crisis management support to Federal, State, and local government entities and private entities that own or operate information systems or networks of information systems to protect from, prevent, mitigate, respond to, and recover from cyber incidents;

''(4) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

''(5) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors on the development and implementation of procedures to support technology neutral real-time information sharing capabilities and mechanisms;

''(6) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors to identify requirements for data

and information formats and accessibility, system interoperability, and redundant systems and alternative capabilities in the event of a disruption in the primary information sharing capabilities and mechanisms at the Center;

''(7) within the scope of relevant treaties, cooperate with international partners to share information and respond to cyber incidents;

''(8) safeguard sensitive cyber threat information from unauthorized disclosure;

''(9) require other Federal civilian agencies to—

''(A) send reports and information to the Center about cyber incidents, threats, and vulnerabilities affecting Federal civilian information systems and critical infrastructure systems and, in the event a private vendor product or service of such an agency is so implicated, the Center shall first notify such private vendor of the vulnerability before further disclosing such information;

''(B) provide to the Center cyber incident detection, analysis, mitigation, and response information; and

''(C) immediately send and disclose to the Center cyber threat information received by such agencies; and

''(10) perform such other duties as the Secretary may require to facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats.

''(e) INTEGRATION AND ANALYSIS.—The Center shall maintain an integration and analysis function, which shall —

''(1) integrate and analyze all cyber threat information received from other Federal agencies, State and local governments, Information Sharing and Analysis Centers, private entities, critical infrastructure owners, and critical infrastructure operators, and share relevant information in near real-time;

''(2) on an ongoing basis, assess and evaluate consequence, vulnerability, and threat information to share with the entities referred to in subsection (a) actionable assessments of critical infrastructure sector risks from cyber incidents and to assist critical infrastructure owners and critical infrastructure operators by making recommendations to facilitate continuous improvements to the security and resil-

iency of the critical infrastructure of the United States;

''(3) facilitate cross-sector integration, identification, and analysis of key interdependencies to prevent related or consequential impacts to other critical infrastructure sectors; and

''(4) collaborate with the Information Sharing and Analysis Centers to tailor the analysis of information to the specific characteristics and risk to a relevant critical infrastructure sector.

''(f) REPORT OF CYBER ATTACKS AGAINST FEDERAL GOVERNMENT NETWORKS.—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report that summarizes major cyber incidents involving Federal civilian agency information systems and provides aggregate statistics on the number of breaches, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedying such breaches.

''(g) REPORT ON THE OPERATIONS OF THE CENTER.—The Secretary, in consultation with the Sector Coordinating Councils and appropriate Federal Government entities, shall submit to the Committee on Homeland Se-

curity of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report on—

''(1) the capability and capacity of the Center to carry out its cybersecurity mission in accordance with this section, and sections 226, 227, 229, 230, 230A, and 230B;

''(2) the extent to which the Department is engaged in information sharing with each critical infrastructure sector designated under section 227(b), including—

''(A) the extent to which each such sector has representatives at the Center; and

''(B) the extent to which critical infrastructure owners and critical infrastructure operators of each critical infrastructure sector participate in information sharing at the Center;

''(3) the volume and range of activities with respect to which the Secretary collaborated with the Sector Coordinating Councils and the Sector-Specific Agencies to promote greater engagement with the Center; and

''(4) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure owner and critical infrastructure operator.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by section 103, is further amended by adding at the end the following new item:

''228. National Cybersecurity and Communications Integration Center.''.

(c) GAO REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States 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 effectiveness of the National Cybersecurity and Communications Integration Center established under section 228 of the Homeland Security Act of 2002, as added by subsection (a) of this section, in carrying out its cybersecurity mission in accordance with this Act and such section 228 and sections 226, 227, 229, 230, 230A, and 230B of the Homeland Security Act of 2002, as added by this Act.

SEC. 105. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102,

103, and 104, is further amended by adding at the end the following new section:

"SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

"(a) IN GENERAL.—The Secretary shall establish Cyber Incident Response Teams to—

"(1) upon request, provide timely technical assistance and crisis management support to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators involving cyber incidents affecting critical infrastructure; and

"(2) upon request, provide actionable recommendations on security and resilience measures and countermeasures to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators prior to, during, and after cyber incidents.

"(b) COORDINATION.—In carrying out subsection (a), the Secretary shall coordinate with the relevant Sector Specific Agencies, if applicable.

"(c) CYBER INCIDENT RESPONSE PLAN.—The Secretary, in coordination with the Sector Coordinating Councils, Information Sharing and Analysis Centers, and Federal, State, and local governments, shall develop, regularly

update, maintain, and exercise a National Cybersecurity Incident Response Plan which shall—

''(1) include effective emergency response plans associated with cyber threats to critical infrastructure, information systems, or networks of information systems; and

''(2) ensure that such National Cybersecurity Incident Response Plan can adapt to and reflect a changing cyber threat environment, and incorporate best practices and lessons learned from regular exercises, training, and after-action reports.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 103 and 104, is further amended by adding at the end the following new item:

''229. Cyber incident response and technical assistance.''.

SEC. 106. ASSESSMENT OF CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 103, 104, and 105, is further amended by adding at the end the following new section:

''SEC. 230. ASSESSMENT OF CYBERSECURITY WORKFORCE.

''(a) ASSESSMENT.—The Secretary, in consultation with relevant private entities, shall regularly assess the readiness and capacity of the workforce of the Department

to meet the needs of the cybersecurity mission of the Department.

''(b) STRATEGY REQUIRED.—Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy designed to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity personnel of the Department. Such strategy shall include a five-year plan on recruitment of personnel for the workforce of the Department, and ten-year projections of the workforce needs of the Department. The Secretary shall submit such strategy to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 103, 104, and 105, is further amended by adding at the end the following new item:

''230. Assessment of cybersecurity workforce.''.

SEC. 107. PERSONNEL AUTHORITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 102, 103, 104, 105, and 106, is further amended by adding at the end the following new section:

"SEC. 230A. PERSONNEL AUTHORITIES.

''(a) IN GENERAL.—

''(1) PERSONNEL AUTHORITIES.—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title 10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary 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 written explanation of such determination. Such authority shall be exercised—

''(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

"(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

"(2) CIVIL SERVICE PROTECTIONS.—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).

"(3) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of the enactment of this section, the Secretary 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 that contains a plan for the use of the authorities provided under this subsection.

"(b) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary 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 detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting

applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

''(c) DEFINITION OF QUALIFIED EMPLOYEE.—In this section, the term 'qualified employee' means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastructure information systems, or networks of either of such systems.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 103, 104, 105, and 106, is further amended by adding at the end the following new item:

''230A. Personnel authorities.''.

SEC. 108. STREAMLINING OF DEPARTMENT CYBERSECURITY ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this Act, be known and designated as the ''Cybersecurity and Infrastructure Protection Directorate''. Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to

be a reference to the Cybersecurity and Infrastructure Protection Directorate of the Department.

(b) SENIOR LEADERSHIP OF THE CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended by adding at the end the following new subparagraphs:

''(K) Under Secretary for Cybersecurity and Infrastructure Protection.

''(L) Deputy Under Secretary for Cybersecurity.

''(M) Deputy Under Secretary for Infrastructure Protection.''.

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred to in subparagraphs (K), (L), and (M) of subsection (a) of section 103 of the Homeland Security Act of 2002 (as added by paragraph (1) of this subsection) as of the date of the enactment of this Act may continue to hold such positions.

(c) REPORT ON IMPROVING THE CAPABILITY AND EFFECTIVENESS OF THE CYBERSECURITY AND COMMUNICATIONS OFFICE.—To improve the operational capability and effectiveness in carrying out the cybersecurity

mission of the Department of Homeland Security, 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—

(1) the feasibility of making the Cybersecurity and Communications Office of the Department an operational component of the Department;

(2) recommendations for restructuring the SAFETY Act Office within the Department to elevate the profile and mission of the Office, including the feasibility of utilizing third-party registrars for improving the throughput and effectiveness of the certification process.

(d) REPORT ON CYBERSECURITY ACQUISITION CAPABILITIES.—The Secretary of Homeland Security shall assess the effectiveness of the Department of Homeland Security's acquisition processes and the use of existing authorities for acquiring cybersecurity technologies to ensure that such processes and authorities are capable of meeting the needs and demands of the Department's cybersecurity mission. Not later than 180 days after the date of the enactment of this Act, the Secretary 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 effectiveness of the Department's acquisition processes for cybersecurity technologies.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102, 103, 104, 105, 106, and 107, is further amended by adding at the end the following new section:

"SEC. 230B. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

"(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Director of the National Institute of Standards and Technology, in collaboration with the Secretary, shall, on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure. The Director, in collaboration with the Secretary—

"(1) shall—

"(A) coordinate closely and continuously with relevant private entities, critical infrastruc-

ture owners and critical infrastructure operators, Sector Coordinating Councils, Information Sharing and Analysis Centers, and other relevant industry organizations, and incorporate industry expertise to the fullest extent possible;

"(B) consult with the Sector Specific Agencies, Federal, State and local governments, the governments of other countries, and international organizations;

"(C) utilize a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by critical infrastructure owners and critical infrastructure operators to help them identify, assess, and manage cyber risks;

"(D) include methodologies to—

"(i) identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

"(ii) protect individual privacy and civil liberties;

"(E) incorporate voluntary consensus standards and industry best practices, and align

with voluntary international standards to the fullest extent possible;

''(F) prevent duplication of existing regulatory processes and prevent conflict with or superseding of existing regulatory requirements and processes; and

''(G) include such other similar and consistent elements as determined necessary; and

''(2) shall not prescribe or otherwise require—

''(A) the use of specific solutions;

''(B) the use of specific information technology products or services; or

''(C) that information technology products or services be designed, developed, or manufactured in a particular manner.

''(b) MEETINGS.—The Secretary shall meet with the Sector Coordinating Council for each critical infrastructure sector designated under section 227(b) on a biannual basis to discuss the cybersecurity threat to critical infrastructure, voluntary activities to address cybersecurity, and ideas to improve the public-private partnership to enhance cybersecurity, in which the Secretary shall—

''(1) provide each Sector Coordinating Council an assessment of the cybersecurity threat to each

critical infrastructure sector designated under section 227(b), including information relating to—

''(A) any actual or assessed cyber threat, including a consideration of adversary capability and intent, preparedness, target attractiveness, and deterrence capabilities;

''(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure;

''(C) the threat to national security caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

''(D) the harm to the economy that would result from an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

''(2) provide recommendations, which may be voluntarily adopted, on ways to improve cybersecurity of critical infrastructure.

''(c) REPORT.—

''(1) IN GENERAL.—Starting 30 days after the end of the fiscal year in which the National Cyberse-

curity and Critical Infrastructure Protection Act of 2013 is enacted 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 Governmental Affairs of the Senate a report on the state of cybersecurity for each critical infrastructure sector designated under section 227(b) based on discussions between the Department and the Sector Coordinating Council in accordance with subsection (b) of this section. The Secretary shall maintain a public copy of each report, and each report may include a non-public annex for proprietary or business-sensitive information. Each report shall include, at a minimum information relating to—

''(A) the risk to each critical infrastructure sector, including known cyber threats, vulnerabilities, and potential consequences;

''(B) the extent and nature of any cybersecurity incidents during the previous year, including the extent to which cyber incidents jeopardized or imminently jeopardized information systems;

''(C) the current status of the voluntary, industry-led set of standards, guidelines, best

practices, methodologies, procedures, and processes to reduce cyber risks within each critical infrastructure sector; and

"(D) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure sector.

"(2) SECTOR COORDINATING COUNCIL RESPONSE.—Before making public and submitting each report required under paragraph (1), the Secretary shall provide a draft of each report to the Sector Coordinating Council for the critical infrastructure sector covered by each such report. The Sector Coordinating Council at issue may provide to the Secretary a written response to such report within 45 days of receiving the draft. If such Sector Coordinating Council provides a written response, the Secretary shall include such written response in the final version of each report required under paragraph (1).

"(d) LIMITATION.—Information shared with or provided to the Director of the National Institute of Standards and Technology or the Secretary for the purpose of the activities under subsections (a) and (b) shall not be used by any Federal, State, or local government depart-

ment or agency to regulate the activity of any private entity.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 102, 103, 104, 105, 106, and 107 is further amended by adding at the end the following new item:

''Sec. 230B. Public-private collaboration on cybersecurity.''.

SEC. 202. SAFETY ACT AND QUALIFYING CYBER INCIDENTS.

(a) IN GENERAL.—The Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (6 U.S.C. 441 et seq.) is amended—

(1) in section 862(b) (6 U.S.C. 441(b))—

(A) in the heading, by striking ''DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES'' and inserting ''DESIGNATION OF ANTI-TERRORISM AND CYBERSECURITY TECHNOLOGIES'';

(B) in the matter preceding paragraph (1), by inserting ''and cybersecurity'' after ''anti-terrorism'';

(C) in paragraphs (3), (4), and (5), by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears; and

(D) in paragraph (7)—

(i) by inserting ''or cybersecurity technology'' after ''Anti-terrorism technology''; and

(ii) by inserting ''or qualifying cyber incidents'' after ''acts of terrorism'';

(2) in section 863 (6 U.S.C. 442)—

(A) by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears;

(B) by inserting ''or qualifying cyber incident'' after ''act of terrorism'' each place it appears; and

(C) by inserting ''or qualifying cyber incidents'' after ''acts of terrorism'' each place it appears;

(3) in section 864 (6 U.S.C. 443)—

(A) by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears; and

(B) by inserting ''or qualifying cyber incident'' after ''act of terrorism'' each place it appears; and

(4) in section 865 (6 U.S.C. 444)—

(A) in paragraph (1)—

(i) in the heading, by inserting ''OR CYBERSECURITY'' after ''ANTI-TERRORISM'';

(ii) by inserting ''or cybersecurity'' after ''anti-terrorism''; and

(iii) by inserting ''or qualifying cyber incident'' after ''acts of terrorism''; and

(B) by adding at the end the following new paragraph:

''(7) QUALIFYING CYBER INCIDENT.—

''(A) IN GENERAL.—The term 'qualifying cyber incident' means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

''(B) REQUIREMENTS.—A qualifying cyber incident meets the requirements of this subparagraph if the incident—

''(i) is unlawful or otherwise exceeds authorized access authority;

''(ii) disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of programmable electronic devices, communication networks, including hardware, software and data that are essential to their reliable operation, electronic storage devices, or any other information system, or the informa-

tion that system controls, processes, stores, or transmits;

''(iii) gains access to an information system or a network of information systems resulting in—

''(I) misappropriation or theft of data, assets, information, or intellectual property;

''(II) corruption of data, assets, information, or intellectual property;

''(III) operational disruption; or

''(IV) an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and

''(iv) causes harm inside or outside the United States that results in material levels of damage, disruption, or casualties severely affecting the United States population, infrastructure, economy, national morale, or Federal, State, local, or tribal government functions.''.

(b) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Science and Technology Directorate of the Depart-

ment of Homeland Security, the Secretary of Homeland Security is authorized to use not less than $20,000,000 for any such year for the Department's SAFETY Act Office.

SEC. 203. PROHIBITION ON NEW REGULATORY AUTHORITY.

This Act and the amendments made by this Act do not—

(1) create or authorize the issuance of any new regulations or additional Federal Government regulatory authority; or

(2) permit regulatory actions that would duplicate, conflict with, or supercede existing regulatory requirements, mandatory standards, or related processes.

SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act. This Act and such amendments shall be carried out using amounts otherwise available for such purposes.

○