# [DISCUSSION DRAFT]

113TH CONGRESS
1ST SESSION

# H. R. _____

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

---

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

---

# A BILL

To amend the Homeland Security Act of 2002 to make certain improvements in the law 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'' or the ''NCCIP Act''.

**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. GOVERNMENT COORDINATED ACTIVITIES WITH RESPECT TO CYBERSECURITY.

The Department of Homeland Security, the Department of Justice, and the Department of Defense shall conduct cybersecurity activities to provide shared situational awareness that enables real-time, integrated and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

# TITLE II—ROLE OF DEPARTMENT OF HOMELAND SECURITY

## SEC. 201. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY PROGRAM.

(a) IN GENERAL.—Section 223 of the Homeland Security Act of 2002 (6 U.S.C. 143) is amended to read as follows:

**"SEC. 223. ENHANCEMENT OF CYBERSECURITY.**

''(a) IN GENERAL.—The Secretary, in collaboration with other appropriate Federal government entities, shall conduct cybersecurity activities to provide shared situational awareness that enables real-time, integrated and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

''(b) RESPONSIBILITIES.—The Secretary shall be responsible for cybersecurity protection, and shall—

''(1) coordinate the national prevention of, protection from, and recovery from cyber incidents;

''(2) direct an entity within the Department to serve as the Federal civilian entity by and among Federal, State, and local governments, private entities, and critical infrastructure sectors that provides multi-directional sharing of real-time, actionable, and relevant cyber threat information; and

''(3) promote a national awareness program to educate and assist private entities, critical infrastructure sectors, and the general public to secure their own information systems.''.

(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 striking the item relating to section 223 and inserting the following new item:

''Sec. 223. 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. 202. 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:

''(18) 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)).

''(19) The term 'critical infrastructure owner' means an entity that owns critical infrastructure.

''(20) The term 'critical infrastructure operator' means an entity that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure, and may include a critical infrastructure owner.

''(21) The term 'cyber incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies related to an information system.

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

''(23) CYBERSECURITY PURPOSE.—

''(A) IN GENERAL.—The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or

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

''(i) a vulnerability of a system or network;

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

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

''(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(24) CYBERSECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

''(i) a vulnerability of a system or network;

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

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a private entity; or

''(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.—Such term does not include a system designed or employed to protect

a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

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

''(26) CYBER THREAT INFORMATION.—

''(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to—

''(i) a vulnerability of a system or network of a government or private entity or utility;

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

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

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

''(B) EXCLUSION.—Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

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

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

operated by another entity on behalf of a Federal agency; and

"(B) does not include—

"(i) a national security system; or

"(ii) information and 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.

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

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity;

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

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

''(29) The term 'information system' means the underlying framework 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.

''(30) The term 'private entity' means any individual or any private company, utility, organization, or corporation, including an officer, employee, or agent thereof.

''(31) 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.

''(32) The term 'shared situational awareness' means an environment where 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. 203. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.**

(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. 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, and critical infrastructure operators to—

''(A) coordinate the overall Federal protection efforts and provide strategic guidance to promote the security and resilience of the Nation's critical infrastructure from cyber threats;

''(B) develop and maintain a coordinated structure and unity of effort across all critical infrastructure sectors recognizing key interdependencies to strengthen and maintain secure, functioning, and resilient critical infrastructure;

''(C) ensure that Department policies and procedures permit critical infrastructure owners and critical infrastructure operators to receive

real-time, actionable, and relevant cyber threat information;

''(D) leverage industry sector-specific expertise to assist in the development of security and resiliency strategies, and ensure that the allocation of resources are cost effective and reduce any burden on critical infrastructure owners and critical infrastructure operators;

''(E) coordinate and facilitate risk management efforts to reduce vulnerabilities, identify and disrupt threats, and minimize consequences to critical infrastructure;

''(F) provide guidance on the use of protective measures and countermeasures to strengthen the security and resilience of the Nation's critical infrastructure; and

''(G) coordinate a research and development strategy for critical infrastructure technologies.

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

''(A) promote a national awareness program and provide useful tools and technical assistance to educate and empower private enti-

ties and individuals to secure their own information systems;

''(B) facilitate expeditious cyber incident response and recovery assistance and provide crisis management and technical assistance to other Federal, State, and local government entities and private entities for cyber incidents affecting critical infrastructure; and

''(C) 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 Nation depends.

''(b) CRITICAL INFRASTRUCTURE SECTORS.—The Secretary shall designate critical infrastructure sectors, the number of which may increase, decrease, or include subdivision of sectors within a sector as the Secretary may determine. To the fullest extent practicable, critical infrastructure owners and critical infrastructure operators shall not be designated into more than one sector. 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) DESIGNATION OF SECTOR-SPECIFIC AGENCIES.—The Secretary, in coordination with the relevant Sector Coordinating Council, shall designate a Federal agency as the Sector-Specific Agency for the sector designated under subsection (b). If the designated Sector-Specific Agency is the Department, for the purposes of this section, the Department will carry out this section on its own. The Secretary, in coordination with the Sector-Specific Agency shall—

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

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

''(3) tailor any policies and procedures to the specific characteristics and risk landscape of the critical infrastructure sector.

''(d) SECTOR COORDINATING COUNCILS.—

''(1) ESTABLISHMENT.—The Secretary shall designate a Sector Coordinating Council for each critical infrastructure sector designated under subsection (b).

''(2) MEMBERSHIP.—The Sector Coordinating Council for a critical infrastructure sector shall be comprised exclusively of critical infrastructure owners, critical infrastructure operators, and representative trade associations for the sector; reflect the unique composition of each sector; and include small, medium, and large critical infrastructure owners, critical infrastructure operators, and representative trade associations. No government entity 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 the primary policy, planning, and communications entity for coordinating with the Department and the Sector-Specific Agency on critical infrastructure protection programs and activities;

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

''(D) coordinate with the Department and the relevant official sector Information Sharing and Analysis Center on the development and implementation of policies and procedures to support technology neutral real-time information sharing capabilities and mechanisms for each sector;

''(E) facilitate inclusive coordination of policy development, strategic planning, exercises and training, and other associated activities and ensure flexibility to apply lessons learned and best practices and to reflect a changing cyber threat environment;

''(F) develop, implement, maintain, and regularly exercise effective emergency response plans associated with cyber incidents to critical infrastructure, systems, networks, functions, or their interconnecting links;

''(G) serve as the strategic communications and coordination point between the sector, the Department, and the Sector-Specific Agency for emergency response and recovery operations; and

''(H) provide input to the Department on infrastructure protection technology gaps to help inform research and development efforts at the Department.

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

''(1) ESTABLISHMENT.—The Secretary shall designate an official sector Information Sharing and Analysis Center for each critical infrastructure sector designated under subsection (b).

''(2) ROLES AND RESPONSIBILITIES.—The official sector Information Sharing and Analysis Center for a critical infrastructure sector shall—

''(A) serve as the primary information sharing entity for a sector, which shall be oper-

ational 24 hours a day, and promote ongoing multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among the sector, the Department, and other official sector Information Sharing and Analysis Centers;

''(B) establish governance and operating procedures to carry out the activities in this subsection;

''(C) coordinate with the Department and the relevant Sector Coordinating Council on the development, integration, and implementation of policies and procedures to support technology neutral real-time information sharing capabilities and mechanisms with the National Cybersecurity and Communications Integration Center designated under section 204;

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

''(E) implement an integration and analysis function to inform sector planning and operational decisions regarding the protection of the sector from cyber incidents;

''(F) provide risk mitigation and cyber incident response capabilities for members within the critical infrastructure sector; and

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

''(f) CLEARANCES.—The Secretary shall expedite the processing of security clearances to appropriate members of the Sector Coordinating Councils and the official Information Sharing and Analysis Centers.

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

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

''(h) PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.—The Secretary shall administer and oversee the operational information security activities and functions to protect and ensure the resiliency of all Federal civilian information systems.

''(1) ROLES AND RESPONSIBILITIES.—The Secretary, in coordination with other Federal 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 to disseminate actionable cyber threat information;

"(D) develop and operate an integrated and consolidated system of intrusion detection, analytics, intrusion prevention, and information sharing capabilities used 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, that may include 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 security 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 designated under section 204 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) develop training requirements 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.

"(2) USE OF CERTAIN COMMUNICATIONS.—Notwithstanding any other provision of law in carrying out subparagraphs (C), (D), (E), (F) in this subsection, the Secretary may acquire, retain, use, and disclose communications and other traffic that are transiting to or from or stored on Federal civilian information systems and deploy countermeasures

with regard to the communications and system traffic.''.

(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. 226. Protection of critical infrastructure and information sharing.''.

**SEC. 204. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 202, is further amended by adding at the end the following new section:

**''SEC. 227. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.**

''(a) ESTABLISHMENT.—There is hereby established in the Department the National Cybersecurity and Communications Integration Center which shall be the civilian Federal entity which shall be an information sharing interface and shall be operational 24 hours a day, to provide shared situational awareness that enables real-time, integrated and operational actions across the Federal Government, and share cyber threat information by and among Federal, State, and local government entities, private entities, and critical infrastructure sectors.

''(b) COMPOSITION.—The Center shall include, but not be limited to, each of the following:

''(1) Official Sector Information Sharing and Analysis Centers designated under section 226(e).

''(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 Nation, 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 Computer Emergency Readiness 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 emergency communications from a cyber incident.

''(6) Such other Federal, State, and local government entities, private entities, or individuals as the Secretary may warrant.

''(c) CYBER INCIDENT.—In the event of a cyber incident, the Secretary may grant Federal, State, and local entities, private entities, or critical infrastructure owners and critical infrastructure operators immediate temporary access to the Center as a situation may warrant.

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

''(1) promote ongoing multi-directional sharing of actionable cyber threat information and analysis on a real-time or near real-time basis as the case may warrant, that includes emerging trends, evolving threats, incident reports, intelligence information, risk assessments, and best practices by and among Federal, State and local governments, private entities, and critical infrastructure sectors;

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

''(3) coordinate the national effort and provide timely technical assistance to Federal, State, and local government entities and private entities who own or operate 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 recognizing key interdependencies to prevent related or consequential impacts to other critical infrastructure sectors;

''(5) coordinate with the Sector Coordinating Councils and the official Information Sharing and Analysis Centers on the development, and implementation of policies and procedures to support technology neutral real-time information sharing capabilities and mechanisms;

''(6) coordinate with the Sector Coordinating Councils and the official Information Sharing and Analysis Centers 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 cyber threat information from unauthorized disclosure;

''(9) require other Federal agencies to—

''(A) send reports and information about cyber incidents, threats, and vulnerabilities affecting Federal civilian information systems to the Center;

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

''(C) immediately send and disclose cyber threat information received by a cyber security provider to the Center; and

''(10) perform such other duties as the Secretary may require relating to the coordination of the national protection of, prevention, mitigation of, and recovery from cyber incidents.

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

''(1) analyze and integrate all information received from other Federal agencies, State and local governments, private entities, and the critical infrastructure sectors, and share such cyber threat information and analysis in near real-time;

''(2) on an ongoing basis, assess and evaluate consequence, vulnerability, and threat information to

share actionable assessments of critical infrastructure sector risks from cyber incidents and to assist critical infrastructure sectors in making continuous improvements to the security and resiliency of the Nation's critical infrastructure;

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

''(4) coordinate with the official Information Sharing and Analysis Centers to tailor the analysis of information to the specific characteristics and risk landscape of a relevant sector.

''(f) INFORMATION SHARING PROCEDURES AND PROTECTIONS.—

''(1) IN GENERAL.—The Center may enter into an information sharing relationship with any private entity for the sharing of cyber threat information for cybersecurity purposes in accordance with this subsection.

''(2) AGREEMENTS.—

''(A) CENTER MEMORANDUM OF UNDERSTANDING.—To enter into an information sharing relationship with the Center under this subsection, a private entity shall enter into a

memorandum of understanding with the Center that sets forth the general terms of the relationship, including all information protections and liability exemptions as set forth in this subsection. A memorandum of understanding described in this paragraph shall be finalized within 72 hours of a request to enter into an information sharing relationship with the Center. The Center Memorandum of Understanding shall be the only agreement required to enter into a formal information sharing relationship with the Center. Any information sharing contractual agreement in effect prior to the date of the enactment of this paragraph is exempt from this paragraph.

''(B) OTHER AGREEMENTS.—Nothing in this paragraph shall preclude the Department or the Center from entering into other information sharing agreements with private entities. All such other agreements shall include all information protections and liability exemptions as set forth in this section and must be negotiated and finalized within 60 days of a request to enter into an agreement.

''(3) INFORMATION SHARING.—

''(A) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, share cyber threat information obtained on its own information system as provided in this subsection.

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

''(C) CLEARANCES.—The Secretary shall expedite the processing of security clearances to appropriate private entities who have entered into an information sharing relationship under this section.

''(D) SAVINGS CLAUSE.—Nothing in this subsection shall limit or modify any information sharing relationship in effect as of the date of the enactment of this section.

''(4) PRIVACY PROTECTIONS FOR INFORMATION SHARING.—

''(A) POLICIES AND PROCEDURES.—The Office of Privacy of the Department on an ongoing basis shall—

''(i) review all policies and procedures governing the sharing of cyber threat information by a private entity with the Center, or by a private entity with another private entity through an official Information Sharing and Analysis Center, to ensure that such policies and procedures are consistent with the Fair Information Practice Principles.; and

''(ii) prepare, as necessary, privacy impact assessments to ensure all relevant constitutional, legal, and privacy protections are being followed.

''(B) OFFICE OF PRIVACY REPORT.—The Office of Privacy of the Department shall prepare an annual report to Congress containing an assessment of the effectiveness of the privacy measures governing the sharing of cyber threat information through the Center and the official Information Sharing and Analysis Centers. Such report shall be made available upon request to the Committee on Homeland Secu-

rity of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

''(5) PROTECTION OF INFORMATION.—

''(A) IN GENERAL.—Any cyber threat information shared under this section shall be used solely for cybersecurity purposes and shall only be further disclosed to any official Information Sharing and Analysis Center or as otherwise expressly agreed to by the Secretary.

''(B) UNFAIR PRACTICES AND ANTITRUST EXEMPTION.—Cyber threat information shared in accordance with this section—

''(i) may not be used by a private entity to gain an unfair competitive advantage to the detriment of a private entity that shared information through the Center or otherwise under this section; and

''(ii) in the case of information shared from one private entity to another private entity through an official Information Sharing and Analysis Center, the sharing of such information shall not be considered a violation of any provision of anti-trust laws.

''(C) FEDERAL GOVERNMENT.—Information shared with the Federal Government through the Center or otherwise under this section—

''(i) is exempt from disclosure under section 552 of title 5, United States Code;

''(ii) shall be considered proprietary information and may not be disclosed to an entity outside the Federal Government unless otherwise expressly authorized by the private entity sharing such information;

''(iii) may not be used by the Federal government for regulatory purposes; and

''(iv) shall be exempt from disclosure under a State, local, or tribal law or regulation that requires public disclosure of information by a public or quasi-public entity.

''(6) FEDERAL PREEMPTION.—This section supercedes any law of a State or political subdivision of a State that restricts or otherwise expressly regulates the sharing of information by a private entity as provided in this section.

''(7) LIABILITY EXEMPTION.—

"(A) IN GENERAL.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against an entity acting in good faith for—

"(i) using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or

"(ii) decisions made for cybersecurity purposes and based on cyber threat information or for sharing such information in accordance with this section.

"(B) LACK OF GOOD FAITH.—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes any act or omission taken with intent to injure, defraud, or otherwise endanger any individual government entity or private entity.

"(C) APPLICABILITY.—This section shall apply to information shared by a private entity to the Center or a private entity to another private entity through an official Information Sharing and Analysis Center.

"(8) STATUTE OF LIMITATIONS.—No action shall lie under this paragraph unless such action is

commenced not later than two years after the date of the alleged violation.

''(9) DEPARTMENT USE OF INFORMATION.—

''(A) CYBERSECURITY PURPOSES.—The Secretary may use cyber threat information shared with the Center in accordance with this section for cybersecurity purposes.

''(B) DEPARTMENTAL CAUSE OF ACTION.—If the Secretary intentionally violates any of the restrictions on the disclosure, use, or protection of information shared by a private entity with the Center in accordance with this section, a cause of action may lie or be maintained by a person in a Federal court.

''(g) SEE SOMETHING, SAY SOMETHING FOR CYBER THREATS.—

''(1) IN GENERAL.—The Secretary shall establish policies and procedures at the Center to encourage and facilitate any private entity or individual, whether or not they have an information sharing relationship with the Center, to report any type of information that may pertain to a cyber threat to critical infrastructure. To the extent practicable, any person should make a good faith effort to share any information that concerns—

''(A) 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;

''(B) a threat to national security caused by the disruption, destruction, or unauthorized use of critical infrastructure; and

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

''(2) APPLICABILITY.—The information sharing protection and liability exemptions provided in this section shall apply to this paragraph.

''(3) SAVINGS CLAUSE.—Nothing in this section shall be construed to require any private entity or individual to share information with the Center.

''(h) ACQUISITION AUTHORITIES.—

''(1) IN GENERAL.—The Center is authorized to use the authorities under subsections (c)(1) and (d)(1)(B) of section 2304 of title 10, United States Code, instead of the authorities under subsections (a)(1) and (b)(2) of section 3304 of title 41, United States Code, subject to all other requirements of sections 3301 and 3304 of title 41, United States Code.

''(2) GUIDELINES.—Not later than 90 days after the date of the enactment of this section, the chief procurement officer of the Department shall issue guidelines for use of the authority under paragraph (1).

''(3) ANNUAL REPORT.—Not later than 60 days after the last day of a fiscal year, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security of the Senate a report on the use of the authority under paragraph (1) during that fiscal year. Each such report shall contain—

''(A) the number of contract actions taken under the authority under such paragraph during the period covered by the report; and

''(B) for each such contract action—

''(i) the total dollar value of the contract action;

''(ii) a summary of the market research conducted by the Center, including a list of all offerors who were considered and those who actually submitted bids, in order to determine that use of the authority was appropriate; and

''(iii) a copy of the justification and approval documents required by section 3304(e) of title 41, United States Code.

''(i) REPORT OF CYBER ATTACKS AGAINST GOVERNMENT NETWORKS.—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 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 the breaches involving Federal civilian information systems. The contents of the report may be provided to Congress through real-time electronic dashboard reporting in lieu of a written document.

''(j) 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 Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report on the capability and capacity of the Center to carry out its cybersecurity mission in accordance with this Act.

''(k) 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 to ensure the participation of all official sector Information Sharing and Analysis Centers in the Center.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by section 202, is further amended by adding at the end the following new item:

''227. 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 of the Senate a report on the effectiveness of the National Cybersecurity and Communications Integration Center established under section 227 of the Homeland Security Act of 2002, as added by subsection (a) to carry out it's cybersecurity mission in accordance with this Act.

**SEC. 205. CYBER INCIDENT RESPONSE TEAMS.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 202

and 203, is further amended by adding at the end the following new section:

**"SEC. 228. CYBER INCIDENT RESPONSE TEAMS.**

''The Secretary shall—

''(1) Provide timely technical assistance and crisis management to Federal, State, and local government entities, and private entities from cyber incidents affecting critical infrastructure;

''(2) Provide actionable recommendations on security and resilience measures and countermeasures to Federal, State, and local government entities, private entities, and the critical infrastructure sectors prior to, during, and after a cyber incident.

''(3) Develop a national cybersecurity incident response plan which shall—

''(A) coordinate with the Sector Coordinating Councils, Federal, State, and local governments, and other relevant entities to annually develop, implement, and exercise the National Cybersecurity Incident Response Plan that details the roles and responsibilities of critical infrastructure owners, critical infrastructure operators, and Federal, State, and local governments to protect from, prevent, mitigate, respond to, and recover from cyber incidents;

''(B) ensure the National Cybersecurity Incident Response Plan is flexible enough to 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 202 and 203, is further amended by adding at the end the following new item:

''228. Cyber incident response teams.''.

**SEC. 206. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 202, 203, and 204, is further amended by adding at the end the following new section:

**''SEC. 229. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

''(a) ASSESSMENT.—The Secretary 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 and maintain a comprehensive workforce strategy designed to enhance the readiness, capacity, training, recruitment, and retention of the cyberse-

curity 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.

''(c) UPDATES.—The Secretary shall update the strategy maintained under subsection (b) as necessary.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 202, 203, and 204, is further amended by adding at the end the following new item:

''229. Assessment of cybersecurity workforce.''.

**SEC. 207. PERSONNEL AUTHORITIES.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 202, 203, 204, 205, and 206 is further amended by adding at the end the following new section:

**''SEC. 229A. PERSONNEL AUTHORITIES.**

''(a) IN GENERAL.—In order to assure that the Department has the necessary resources to carry out the mission of securing Federal civilian information 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 positions, 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 Representa-

tives 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 202, 203, and 204, is further amended by adding at the end the following new item:

''229A. Personnel authorities.''.

**SEC. 208. 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 such Directorate in any law, regulation, map, document, record, or other paper of the United States shall be considered to be a reference to the Cybersecurity and Infrastructure Protection Directorate.

(b) SENIOR LEADERSHIP OF CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—After the date of the enactment of this Act, there shall be no more than three senior leadership positions in the Cybersecurity and Infrastructure Protection Directorate, including one Under Secretary.

(c) REPORT TO CONGRESS.—To improve the operational capability and effectiveness in carrying out the cybersecurity mission of the Department, the Secretary of Homeland Security shall submit to Congress a report on—

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

(2) recommendations for restructuring the SAFETY Act office within the Department to elevate the profile and mission of the office. The report shall also provide an analysis on the feasibility of utilizing third-party registrars for improving the throughput and effectiveness of the certification process.

# TITLE III—INDUSTRY-LED INITIATIVES TO ADDRESS VULNERABILITIES AND GAPS IN CYBERSECURITY

## SEC. 301. INDUSTRY-LED INITIATIVES TO ADDRESS VULNERABILITIES AND GAPS IN CYBERSECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 202, 203, 204, 205, 206, and 207 is further amended by adding at the end the following new section:

**"SEC. 229B. INDUSTRY-LED INITIATIVES TO ADDRESS VULNERABILITIES IN CYBERSECURITY.**

"(a) INDUSTRY LED INITIATIVES TO ESTABLISH CYBERSECURITY GUIDELINES.—The Sector Coordinating Council for each critical infrastructure sector established under section 226 shall meet no less than six times per year to continually address vulnerabilities and gaps in cybersecurity across the relevant sector. Such meetings shall be conducted to—

"(1) assess, on an ongoing basis, the state of cybersecurity for the relevant critical infrastructure sector to determine guidelines for the critical infrastructure sector, taking into consideration cyber threats, vulnerabilities, and risks, including—

"(A) the actual or assessed 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 a disruption, destruction, or unauthorized use of critical infrastructure;

"(C) the threat to national security caused by the disruption, destruction or unauthorized use of critical infrastructure; and

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

''(2) develop guidelines to mitigate cyber risks for the critical infrastructure sector, taking into consideration—

''(A) current Federal and State regulations, risk management determinations, recognized industry and relevant government best practices and any other relevant information to enhance and address vulnerabilities and gaps in cybersecurity for the critical infrastructure sector;

''(B) consultations with cybersecurity experts and institutions;

''(C) development of cybersecurity guidelines tailored to the size and scope of an entity within a sector;

''(D) neutrality of technology; and

''(E) harmonization with international standards to the greatest extent practicable;

''(3) determine, on an ongoing basis, whether enhancements to cybersecurity guidelines are necessary, and if so, ensure flexibility to reflect a changing cyber threat environment; and

''(4) encourage private entities within the critical infrastructure sector to voluntarily adopt cybersecurity guidelines developed by the Sector Coordinating Council for a critical infrastructure sector.

''(b) INDUSTRY-LED ENFORCEMENT OF GUIDELINES.—

''(1) IN GENERAL.—The Sector Coordinating Councils shall coordinate efforts across the sector to encourage the industry-led enforcement by the sector of voluntarily adopted cybersecurity guidelines to ensure the mitigation of risks for cybersecurity and the hardening of critical infrastructure sector wide.

''(2) THIRD PARTY TECHNICAL ASSISTANCE AND VOLUNTARY ASSESSMENTS.—The Sector Coordinating Councils may enter into agreements with qualified third party private entities to—

''(A) provide technical assistance to private entities that seek assistance in adopting the cybersecurity guidelines established by the Sector Coordinating Council; and

''(B) conduct assessments to assess whether a private entity which has voluntarily adopted cybersecurity guidelines is meeting the cy-

bersecurity guidelines established by the Sector Coordinating Council.

''(c) QUARTERLY COLLABORATION MEETINGS.—The Sector Coordinating Council for each critical infrastructure sector shall meet with the Department on a quarterly basis to—

''(1) discuss efforts being taken by the critical infrastructure sector to address vulnerabilities and gaps in cybersecurity across the sector;

''(2) discuss the state of cybersecurity for the critical infrastructure sector, taking into consideration cyber threats, vulnerabilities, and risks;

''(3) discuss the Department's efforts to protect critical infrastructure as set forth in section 226;

''(4) afford the Secretary an opportunity to understand the cybersecurity guidelines established by the Sector Coordinating Council to address vulnerabilities and gaps in cybersecurity;

''(5) discuss efforts being taken by the critical infrastructure sector to encourage and enforce the voluntary adoption of cybersecurity guidelines established by the Sector Coordinating Council across the sector; and

''(6) share information and ideas to ensure greater cybersecurity for the sector.

''(d) REPORT TO CONGRESS.—

''(1) IN GENERAL.—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 an annual report on the state of cybersecurity for each critical infrastructure sector based on discussions between the Department and the Sector Coordinating Council from the quarterly collaborations meeting under subsection (c). The Secretary shall maintain a copy of the report on the Internet website of the Department.

''(2) SECTOR COORDINATING COUNCIL RESPONSE.—Before making public and submitting the report to the Committees under paragraph (1), the Secretary shall provide a draft of the report to the Sector Coordinating Council for the critical infrastructure sector covered by the report. The Sector Coordinating Council shall provide to the Secretary a written response to the report within 45 days of receiving the draft. The Secretary shall include the written response of the Sector Coordinating Council in the final report submitted under paragraph (1).

''(e) SAVINGS CLAUSE.—Nothing in this section shall be interpreted to create any new regulations, additional

Federal Government regulatory authority, or permit the Federal Government to adopt the cybersecurity guidelines established by a Sector Coordinating Council for regulatory purposes.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act, as amended by sections 202, 203, 204, 205, and 206 is further amended by adding at the end the following new item:

''229B. Industry-led initiatives to address vulnerabilities in cybersecurity.''.

**SEC. 302. SAFETY ACT AND SIGNIFICANT 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—

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

(B) in subsection (b) in paragraphs (3), (4), and (5), by striking ''anti-terrorism'' each place that such appears and inserting ''anti-terrorism or cybersecurity'';

(C) in paragraph (7)—

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

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

(2) in section 863 (6 U.S.C. 442)—

(A) by striking ''anti-terrorism'' each place that such appears and inserting ''anti-terrorism or cybersecurity'';

(B) by striking ''act of terrorism'' each place that such appears and inserting ''act of terrorism or significant cyber incident''; and

(C) by striking ''acts of terrorism'' each place that such appears and inserting ''acts of terrorism or significant cyber incidents'';

(3) in section 864 (6 U.S.C. 443)—

(A) by striking ''anti-terrorism'' each place that such appears and inserting ''anti-terrorism or cybersecurity''; and

(B) by striking ''act of terrorism'' each place that such appears and inserting ''act of terrorism or significant cyber incident''; and

(4) in section 865 (6 U.S.C. 444)—

(A) in paragraph (1) by inserting ''or cybersecurity'' after ''anti-terrorism''; and

(B) by inserting at the end the following new paragraphs:

''(7) SIGNIFICANT CYBER INCIDENT.—

''(A) IN GENERAL.—The term 'significant 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 significant cyber incident meets the requirements of this subparagraph if the attack—

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

''(ii)(I) attempts to or actually 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 device, or any other electronic information system or the information that system controls, processes, stores, or transmits electronic information, including for any information system or component thereof

used to operate covered critical infrastructure; or

''(II) results in the theft or misappropriation in electronic or printed form of private or government information, intellectual property, or personally identifiable information; and

''(iii) causes material harm or results in material economic loss to a person, property, or entity, in or outside the United States.

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

''(A) a significant loss of life;

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

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

''(ii) the sustained disruption of financial systems that would lead to long term

catastrophic economic damage to the United States;

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

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

(b) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Science and Technology Directorate, the Secretary is authorized to use not less than $20,000,000 for any such year for the Department's SAFETY Act office.