

[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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “National Cybersecurity
5 and Critical Infrastructure Protection Act of 2013” or the
6 “NCCIP Act”.

1 **SEC. 2. TABLE OF CONTENTS.**

2 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

Sec. 101. Government coordinated activities with respect to cybersecurity.

TITLE II—ROLE OF DEPARTMENT OF HOMELAND SECURITY

- Sec. 201. Department of Homeland Security cybersecurity program.
- Sec. 202. Homeland Security Act of 2002 definitions.
- Sec. 203. Protection of Critical Infrastructure and Information Sharing.
- Sec. 204. National Cybersecurity and Communications Integration Center.
- Sec. 205. Cyber incident response teams.
- Sec. 206. Assessment of cybersecurity workforce.
- Sec. 207. Personnel authorities.
- Sec. 208. Streamlining of Department cybersecurity organization.

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

- Sec. 301. Industry-led initiatives to address vulnerabilities in cybersecurity.
- Sec. 302. SAFETY Act and significant cyber incidents.

3 **TITLE I—SECURING THE NATION**
4 **AGAINST CYBER ATTACK**

5 **SEC. 101. GOVERNMENT COORDINATED ACTIVITIES WITH**
6 **RESPECT TO CYBERSECURITY.**

7 The Department of Homeland Security, the Depart-
8 ment of Justice, and the Department of Defense shall con-
9 duct cybersecurity activities to provide shared situational
10 awareness that enables real-time, integrated and oper-
11 ational actions to protect from, prevent, mitigate, respond
12 to, and recover from cyber incidents.

1 **TITLE II—ROLE OF DEPART-**
2 **MENT OF HOMELAND SECUR-**
3 **RITY**

4 **SEC. 201. DEPARTMENT OF HOMELAND SECURITY CYBER-**
5 **SECURITY PROGRAM.**

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

9 **“SEC. 223. ENHANCEMENT OF CYBERSECURITY.**

10 “(a) IN GENERAL.—The Secretary, in collaboration
11 with other appropriate Federal government entities, shall
12 conduct cybersecurity activities to provide shared situa-
13 tional awareness that enables real-time, integrated and
14 operational actions to protect from, prevent, mitigate, re-
15 spond to, and recover from cyber incidents.

16 “(b) RESPONSIBILITIES.—The Secretary shall be re-
17 sponsible for cybersecurity protection, and shall—

18 “(1) coordinate the national prevention of, pro-
19 tection from, and recovery from cyber incidents;

20 “(2) direct an entity within the Department to
21 serve as the Federal civilian entity by and among
22 Federal, State, and local governments, private enti-
23 ties, and critical infrastructure sectors that provides
24 multi-directional sharing of real-time, actionable,
25 and relevant cyber threat information; and

1 “(3) promote a national awareness program to
2 educate and assist private entities, critical infra-
3 structure sectors, and the general public to secure
4 their own information systems.”.

5 (b) CLERICAL AMENDMENTS.—

6 (1) SUBTITLE HEADING.—The heading for sub-
7 title C of title II of such Act is amended to read as
8 follows:

9 **“Subtitle C—Cybersecurity and**
10 **Information Sharing”.**

11 (2) TABLE OF CONTENTS.—The table of con-
12 tents in section 1(b) of such Act is amended—

13 (A) by striking the item relating to section
14 223 and inserting the following new item:

“Sec. 223. Enhancement of cybersecurity.”; and

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

“Subtitle C—Cybersecurity and Information Sharing”.

18 **SEC. 202. HOMELAND SECURITY ACT OF 2002 DEFINITIONS.**

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

22 “(18) The term ‘critical infrastructure’ has the
23 meaning given that term in section 1016(e) of the
24 USA Patriot Act (42 U.S.C. 5195c(e)).

1 “(19) The term ‘critical infrastructure owner’
2 means an entity that owns critical infrastructure.

3 “(20) The term ‘critical infrastructure operator’
4 means an entity that manages, runs, or operates, in
5 whole or in part, the day-to-day operations of critical
6 infrastructure, and may include a critical infrastruc-
7 ture owner.

8 “(21) The term ‘cyber incident’ means an oc-
9 currence that—

10 “(A) actually or imminently jeopardizes,
11 without lawful authority, the integrity, con-
12 fidentiality, or availability of information or an
13 information system; or

14 “(B) constitutes a violation or imminent
15 threat of violation of law, security policies, secu-
16 rity procedures, or acceptable use policies re-
17 lated to an information system.

18 “(22) The term ‘cybersecurity provider’ means
19 a non-Federal entity that provides goods or services
20 intended to be used for cybersecurity purposes.

21 “(23) CYBERSECURITY PURPOSE.—

22 “(A) IN GENERAL.—The term ‘cybersecu-
23 rity purpose’ means the purpose of ensuring the
24 integrity, confidentiality, or availability of, or

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

3 “(i) a vulnerability of a system or net-
4 work;

5 “(ii) a threat to the integrity, con-
6 fidentiality, or availability of a system or
7 network or any information stored on proc-
8 essed on, or transiting such a system or
9 network;

10 “(iii) efforts to deny access to or de-
11 grade, disrupt, or destroy a system or net-
12 work; or

13 “(iv) efforts to gain unauthorized ac-
14 cess to a system or network, including to
15 gain such unauthorized access for the pur-
16 pose of exfiltrating information stored on,
17 processed on, or transiting a system or
18 network.

19 “(B) EXCLUSION.—Such term does not in-
20 clude the purpose of protecting a system or net-
21 work from efforts to gain unauthorized access
22 to such system or network that solely involve
23 violations of consumer terms of service or con-
24 sumer licensing agreements and do not other-
25 wise constitute unauthorized access.

1 “(24) CYBERSECURITY SYSTEM.—

2 “(A) IN GENERAL.—The term ‘cybersecu-
3 rity system’ means a system designed or em-
4 ployed to ensure the integrity, confidentiality,
5 or availability of, or safeguard, a system or net-
6 work, including protecting a system or network
7 from—

8 “(i) a vulnerability of a system or net-
9 work;

10 “(ii) a threat to the integrity, con-
11 fidentiality, or availability of a system or
12 network or any information stored on,
13 processed on, or transiting such a system
14 or network;

15 “(iii) efforts to deny access to or de-
16 grade, disrupt, or destroy a system or net-
17 work of a private entity; or

18 “(iv) efforts to gain unauthorized ac-
19 cess to a system or network, including to
20 gain such unauthorized access for the pur-
21 pose of exfiltrating information stored on,
22 processed on, or transiting a system or
23 network.

24 “(B) EXCLUSION.—Such term does not in-
25 clude a system designed or employed to protect

1 a system or network from efforts to gain unau-
2 thorized access to such system or network that
3 solely involve violations of consumer terms of
4 service or consumer licensing agreements and
5 do not otherwise constitute unauthorized access.

6 “(25) The term ‘cyber threat’ means any action
7 that may result in unauthorized access to,
8 exfiltration of, manipulation of, harm of, or impair-
9 ment to the integrity, confidentiality, or availability
10 of an information system or information that is
11 stored on, processed by, or transiting an information
12 system.

13 “(26) CYBER THREAT INFORMATION.—

14 “(A) IN GENERAL.—The term ‘cyber
15 threat information’ means information directly
16 pertaining to—

17 “(i) a vulnerability of a system or net-
18 work of a government or private entity or
19 utility;

20 “(ii) a threat to the integrity, con-
21 fidentiality, or availability of a system or
22 network of a government or private entity
23 or utility or any information stored on,
24 processed on, or transiting such a system
25 or network;

1 “(iii) efforts to deny access to or de-
2 grade, disrupt, or destroy a system or net-
3 work of a government or private entity or
4 utility; or

5 “(iv) efforts to gain unauthorized ac-
6 cess to a system or network of a govern-
7 ment or private entity or utility, including
8 to gain such unauthorized access for the
9 purpose of exfiltrating information stored
10 on, processed on, or transiting a system or
11 network of a government or private entity
12 or utility.

13 “(B) EXCLUSION.—Such term does not in-
14 clude information pertaining to efforts to gain
15 unauthorized access to a system or network of
16 a government or private entity or utility that
17 solely involve violations of consumer terms of
18 service or consumer licensing agreements and
19 do not otherwise constitute unauthorized access.

20 “(27) The term ‘Federal civilian information
21 systems’—

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

1 operated by another entity on behalf of a Fed-
2 eral agency; and

3 “(B) does not include—

4 “(i) a national security system; or

5 “(ii) information and information sys-
6 tems that are owned, operated, controlled,
7 or licensed solely for use by, or on behalf
8 of, the Department of Defense, a military
9 department, or an element of the intel-
10 ligence community.

11 “(28) The term ‘information security’ means
12 the protection of information and information sys-
13 tems from unauthorized access, use, disclosure, dis-
14 ruption, modification, or destruction in order to pro-
15 vide—

16 “(A) integrity, which means guarding
17 against improper information modification or
18 destruction, and includes ensuring nonrepudi-
19 ation and authenticity;

20 “(B) confidentiality, which means pre-
21 serving authorized restrictions on access and
22 disclosure, including means for protecting per-
23 sonal privacy and proprietary information; and

1 “(C) availability, which means ensuring
2 timely and reliable access to and use of infor-
3 mation.

4 “(29) The term ‘information system’ means the
5 underlying framework used to process, transmit, re-
6 ceive, or store information electronically, including
7 programmable electronic devices, communications
8 networks, and industrial or supervisory control sys-
9 tems and any associated hardware, software, or
10 data.

11 “(30) The term ‘private entity’ means any indi-
12 vidual or any private company, utility, organization,
13 or corporation, including an officer, employee, or
14 agent thereof.

15 “(31) The term ‘protected private entity’ means
16 an entity, other than an individual, that enters into
17 a contract with a cybersecurity provider for goods
18 and services to be used for cybersecurity purposes.

19 “(32) The term ‘shared situational awareness’
20 means an environment where cyber threat informa-
21 tion is shared in real time between all designated
22 Federal cyber operations centers to provide action-
23 able information about all known cyber threats.”.

1 **SEC. 203. PROTECTION OF CRITICAL INFRASTRUCTURE**
2 **AND INFORMATION SHARING.**

3 (a) IN GENERAL.—Subtitle C of title II of the Home-
4 land Security Act of 2002 is amended by adding at the
5 end the following new section:

6 **“SEC. 226. PROTECTION OF CRITICAL INFRASTRUCTURE**
7 **AND INFORMATION SHARING.**

8 “(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

9 “(1) IN GENERAL.—The Secretary shall coordi-
10 nate, on an ongoing basis, with Federal, State, and
11 local governments, critical infrastructure owners,
12 and critical infrastructure operators to—

13 “(A) coordinate the overall Federal protec-
14 tion efforts and provide strategic guidance to
15 promote the security and resilience of the Na-
16 tion’s critical infrastructure from cyber threats;

17 “(B) develop and maintain a coordinated
18 structure and unity of effort across all critical
19 infrastructure sectors recognizing key inter-
20 dependencies to strengthen and maintain se-
21 cure, functioning, and resilient critical infra-
22 structure;

23 “(C) ensure that Department policies and
24 procedures permit critical infrastructure owners
25 and critical infrastructure operators to receive

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

3 “(D) leverage industry sector-specific ex-
4 pertise to assist in the development of security
5 and resiliency strategies, and ensure that the
6 allocation of resources are cost effective and re-
7 duce any burden on critical infrastructure own-
8 ers and critical infrastructure operators;

9 “(E) coordinate and facilitate risk manage-
10 ment efforts to reduce vulnerabilities, identify
11 and disrupt threats, and minimize consequences
12 to critical infrastructure;

13 “(F) provide guidance on the use of pro-
14 tective measures and countermeasures to
15 strengthen the security and resilience of the
16 Nation’s critical infrastructure; and

17 “(G) coordinate a research and develop-
18 ment strategy for critical infrastructure tech-
19 nologies.

20 “(2) ADDITIONAL RESPONSIBILITIES.—The
21 Secretary shall—

22 “(A) promote a national awareness pro-
23 gram and provide useful tools and technical as-
24 sistance to educate and empower private enti-

1 ties and individuals to secure their own infor-
2 mation systems;

3 “(B) facilitate expeditious cyber incident
4 response and recovery assistance and provide
5 crisis management and technical assistance to
6 other Federal, State, and local government enti-
7 ties and private entities for cyber incidents af-
8 fecting critical infrastructure; and

9 “(C) engage with international partners to
10 strengthen the security and resilience of domes-
11 tic critical infrastructure and critical infrastruc-
12 ture located outside of the United States upon
13 which the Nation depends.

14 “(b) CRITICAL INFRASTRUCTURE SECTORS.—The
15 Secretary shall designate critical infrastructure sectors,
16 the number of which may increase, decrease, or include
17 subdivision of sectors within a sector as the Secretary may
18 determine. To the fullest extent practicable, critical infra-
19 structure owners and critical infrastructure operators
20 shall not be designated into more than one sector. The
21 critical infrastructure sectors designated under this sub-
22 section may include the following:

23 “(1) Chemical.

24 “(2) Commercial facilities.

25 “(3) Communications.

- 1 “(4) Critical manufacturing.
- 2 “(5) Dams.
- 3 “(6) Defense Industrial Base.
- 4 “(7) Emergency services.
- 5 “(8) Energy.
- 6 “(9) Financial services.
- 7 “(10) Food and agriculture.
- 8 “(11) Government facilities.
- 9 “(12) Healthcare and public health.
- 10 “(13) Information technology.
- 11 “(14) Nuclear reactors, materials, and waste.
- 12 “(15) Transportation systems.
- 13 “(16) Water and wastewater systems.
- 14 “(17) Such other sectors as the Secretary de-
- 15 termines appropriate.
- 16 “(c) DESIGNATION OF SECTOR-SPECIFIC AGEN-
- 17 CIES.—The Secretary, in coordination with the relevant
- 18 Sector Coordinating Council, shall designate a Federal
- 19 agency as the Sector-Specific Agency for the sector des-
- 20 ignated under subsection (b). If the designated Sector-
- 21 Specific Agency is the Department, for the purposes of
- 22 this section, the Department will carry out this section on
- 23 its own. The Secretary, in coordination with the Sector-
- 24 Specific Agency shall—

1 “(1) support the security and resilience pro-
2 grams and activities of the critical infrastructure
3 sector in accordance with this Act;

4 “(2) provide institutional knowledge and spe-
5 cialized expertise to the critical infrastructure sector;
6 and

7 “(3) tailor any policies and procedures to the
8 specific characteristics and risk landscape of the
9 critical infrastructure sector.

10 “(d) SECTOR COORDINATING COUNCILS.—

11 “(1) ESTABLISHMENT.—The Secretary shall
12 designate a Sector Coordinating Council for each
13 critical infrastructure sector designated under sub-
14 section (b).

15 “(2) MEMBERSHIP.—The Sector Coordinating
16 Council for a critical infrastructure sector shall be
17 comprised exclusively of critical infrastructure own-
18 ers, critical infrastructure operators, and representa-
19 tive trade associations for the sector; reflect the
20 unique composition of each sector; and include
21 small, medium, and large critical infrastructure own-
22 ers, critical infrastructure operators, and representa-
23 tive trade associations. No government entity shall
24 be a member of the Sector Coordinating Council.

1 “(3) ROLES AND RESPONSIBILITIES.—The Sec-
2 tor Coordinating Council for a critical infrastructure
3 sector shall—

4 “(A) serve as the primary policy, planning,
5 and communications entity for coordinating
6 with the Department and the Sector-Specific
7 Agency on critical infrastructure protection pro-
8 grams and activities;

9 “(B) establish governance and operating
10 procedures, and designate a chairperson for the
11 sector to carry out the activities in this sub-
12 section;

13 “(D) coordinate with the Department and
14 the relevant official sector Information Sharing
15 and Analysis Center on the development and
16 implementation of policies and procedures to
17 support technology neutral real-time informa-
18 tion sharing capabilities and mechanisms for
19 each sector;

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

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

6 “(G) serve as the strategic communications
7 and coordination point between the sector, the
8 Department, and the Sector-Specific Agency for
9 emergency response and recovery operations;
10 and

11 “(H) provide input to the Department on
12 infrastructure protection technology gaps to
13 help inform research and development efforts at
14 the Department.

15 “(e) SECTOR INFORMATION SHARING AND ANALYSIS
16 CENTERS.—

17 “(1) ESTABLISHMENT.—The Secretary shall
18 designate an official sector Information Sharing and
19 Analysis Center for each critical infrastructure sec-
20 tor designated under subsection (b).

21 “(2) ROLES AND RESPONSIBILITIES.—The offi-
22 cial sector Information Sharing and Analysis Center
23 for a critical infrastructure sector shall—

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

1 ational 24 hours a day, and promote ongoing
2 multi-directional sharing of real-time, relevant,
3 and actionable cyber threat information and
4 analysis by and among the sector, the Depart-
5 ment, and other official sector Information
6 Sharing and Analysis Centers;

7 “(B) establish governance and operating
8 procedures to carry out the activities in this
9 subsection;

10 “(C) coordinate with the Department and
11 the relevant Sector Coordinating Council on the
12 development, integration, and implementation
13 of policies and procedures to support technology
14 neutral real-time information sharing capabili-
15 ties and mechanisms with the National Cyberse-
16 curity and Communications Integration Center
17 designated under section 204;

18 “(D) combine consequence, vulnerability,
19 and threat information to share actionable as-
20 sessments of sector risks from cyber incidents;

21 “(E) implement an integration and anal-
22 ysis function to inform sector planning and
23 operational decisions regarding the protection of
24 the sector from cyber incidents;

1 “(F) provide risk mitigation and cyber in-
2 cident response capabilities for members within
3 the critical infrastructure sector; and

4 “(G) safeguard cyber threat information
5 from unauthorized disclosure.

6 “(f) CLEARANCES.—The Secretary shall expedite the
7 processing of security clearances to appropriate members
8 of the Sector Coordinating Councils and the official Infor-
9 mation Sharing and Analysis Centers.

10 “(g) PUBLIC-PRIVATE COLLABORATION.—The Sec-
11 retary, in collaboration with the Sector-Specific Agencies
12 designated under subsection (c), the Sector Coordinating
13 Councils designated under subsection (d), and the critical
14 infrastructure sectors designated under subsection (b),
15 shall—

16 “(1) conduct an analysis and review of the ex-
17 isting public-private partnership model and evaluate
18 how the model between the Department and critical
19 infrastructure owners and critical infrastructure op-
20 erators can be improved to ensure the Department,
21 critical infrastructure owners, and critical infrastruc-
22 ture operators are equal partners and regularly col-
23 laborate on all programs and activities of the De-
24 partment to protect critical infrastructure; and

1 “(2) develop policies and procedures to ensure
2 continuous, collaborative, and effective interactions
3 between the Department, critical infrastructure own-
4 ers, and critical infrastructure operators.

5 “(h) PROTECTION OF FEDERAL CIVILIAN INFORMA-
6 TION SYSTEMS.—The Secretary shall administer and over-
7 see the operational information security activities and
8 functions to protect and ensure the resiliency of all Fed-
9 eral civilian information systems.

10 “(1) ROLES AND RESPONSIBILITIES.—The Sec-
11 retary, in coordination with other Federal agencies,
12 shall—

13 “(A) develop, issue, and oversee the imple-
14 mentation and compliance of all operational in-
15 formation security policies and procedures to
16 protect and ensure the resiliency of Federal ci-
17 vilian information systems;

18 “(B) administer Federal government-wide
19 efforts to develop and provide adequate, risk-
20 based, cost-effective, and technology neutral in-
21 formation security capabilities;

22 “(C) establish and sustain continuous
23 diagnostics systems for Federal civilian infor-
24 mation systems to aggregate data and to dis-
25 seminate actionable cyber threat information;

1 “(D) develop and operate an integrated
2 and consolidated system of intrusion detection,
3 analytics, intrusion prevention, and information
4 sharing capabilities used to defend Federal ci-
5 vilian information systems from cyber threats;

6 “(E) develop and conduct targeted risk as-
7 sessments and operational evaluations of Fed-
8 eral civilian information systems, in consulta-
9 tion with government and private entities that
10 own and operate such information systems, that
11 may include threat, vulnerability, and impact
12 assessments and penetration testing;

13 “(F) develop and provide technical assist-
14 ance and cyber incident response capabilities to
15 secure and ensure the resilience of Federal civil-
16 ian information systems;

17 “(G) review annually the operational infor-
18 mation security activities and functions of each
19 of the Federal civilian agencies;

20 “(H) develop minimum technology neutral
21 operational requirements for network and secu-
22 rity operations centers to facilitate the protec-
23 tion of all Federal civilian information systems;

24 “(I) develop reporting requirements, con-
25 sistent with relevant law, to ensure the National

1 Cybersecurity and Communications Integration
2 Center designated under section 204 receives all
3 actionable cyber threat information identified
4 on Federal civilian information systems;

5 “(J) develop technology-neutral perform-
6 ance requirements and metrics for the security
7 of Federal civilian information systems;

8 “(K) develop training requirements to en-
9 sure that Federal civilian agencies are able to
10 fully and timely comply with policies and proce-
11 dures issued by the Secretary under this sub-
12 section; and

13 “(L) develop training requirements regard-
14 ing privacy, civil rights, civil liberties, and infor-
15 mation oversight for information security em-
16 ployees who operate Federal civilian informa-
17 tion systems.

18 “(2) USE OF CERTAIN COMMUNICATIONS.—
19 Notwithstanding any other provision of law in car-
20 rying out subparagraphs (C), (D), (E), (F) in this
21 subsection, the Secretary may acquire, retain, use,
22 and disclose communications and other traffic that
23 are transiting to or from or stored on Federal civil-
24 ian information systems and deploy countermeasures

1 with regard to the communications and system traf-
2 fic.”.

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

“Sec. 226. Protection of critical infrastructure and information sharing.”.

7 **SEC. 204. NATIONAL CYBERSECURITY AND COMMUNICA-**
8 **TIONS INTEGRATION CENTER.**

9 (a) IN GENERAL.—Subtitle C of title II of the Home-
10 land Security Act of 2002, as amended by section 202,
11 is further amended by adding at the end the following new
12 section:

13 **“SEC. 227. NATIONAL CYBERSECURITY AND COMMUNICA-**
14 **TIONS INTEGRATION CENTER.**

15 “(a) ESTABLISHMENT.—There is hereby established
16 in the Department the National Cybersecurity and Com-
17 munications Integration Center which shall be the civilian
18 Federal entity which shall be an information sharing inter-
19 face and shall be operational 24 hours a day, to provide
20 shared situational awareness that enables real-time, inte-
21 grated and operational actions across the Federal Govern-
22 ment, and share cyber threat information by and among
23 Federal, State, and local government entities, private enti-
24 ties, and critical infrastructure sectors.

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

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

5 “(2) The Multi-State Information Sharing and
6 Analysis Center to collaborate with State and local
7 governments.

8 “(3) The United States Computer Emergency
9 Readiness Team to coordinate cyber threat informa-
10 tion sharing, proactively manage cyber risks to the
11 Nation, collaboratively respond to cyber incidents,
12 provide technical assistance to information system
13 owners and operators, and disseminate timely notifi-
14 cations regarding current and potential cyber threats
15 and vulnerabilities.

16 “(4) The Industrial Control System Computer
17 Emergency Readiness Team to coordinate with in-
18 dustrial control systems owners and operators and
19 share industrial control systems-related security inci-
20 dents and mitigation measures.

21 “(5) The National Coordinating Center for
22 Telecommunications to coordinate the protection, re-
23 sponse, and recovery of emergency communications
24 from a cyber incident.

1 “(6) Such other Federal, State, and local gov-
2 ernment entities, private entities, or individuals as
3 the Secretary may warrant.

4 “(c) CYBER INCIDENT.—In the event of a cyber inci-
5 dent, the Secretary may grant Federal, State, and local
6 entities, private entities, or critical infrastructure owners
7 and critical infrastructure operators immediate temporary
8 access to the Center as a situation may warrant.

9 “(d) ROLES AND RESPONSIBILITIES.—The Center
10 shall—

11 “(1) promote ongoing multi-directional sharing
12 of actionable cyber threat information and analysis
13 on a real-time or near real-time basis as the case
14 may warrant, that includes emerging trends, evol-
15 ving threats, incident reports, intelligence informa-
16 tion, risk assessments, and best practices by and
17 among Federal, State and local governments, private
18 entities, and critical infrastructure sectors;

19 “(2) coordinate with other Federal agencies to
20 streamline and reduce redundant reporting of cyber
21 threat information;

22 “(3) coordinate the national effort and provide
23 timely technical assistance to Federal, State, and
24 local government entities and private entities who
25 own or operate information systems to protect from,

1 prevent, mitigate, respond to, and recover from
2 cyber incidents;

3 “(4) facilitate cross sector coordination and
4 sharing of cyber threat information recognizing key
5 interdependencies to prevent related or consequential
6 impacts to other critical infrastructure sectors;

7 “(5) coordinate with the Sector Coordinating
8 Councils and the official Information Sharing and
9 Analysis Centers on the development, and implemen-
10 tation of policies and procedures to support tech-
11 nology neutral real-time information sharing capa-
12 bilities and mechanisms;

13 “(6) coordinate with the Sector Coordinating
14 Councils and the official Information Sharing and
15 Analysis Centers to identify requirements for data
16 and information formats and accessibility, system
17 interoperability, and redundant systems and alter-
18 native capabilities in the event of a disruption in the
19 primary information sharing capabilities and mecha-
20 nisms at the Center;

21 “(7) within the scope of relevant treaties, co-
22 operate with international partners to share infor-
23 mation and respond to cyber incidents;

24 “(8) safeguard cyber threat information from
25 unauthorized disclosure;

1 “(9) require other Federal agencies to—

2 “(A) send reports and information about
3 cyber incidents, threats, and vulnerabilities af-
4 fecting Federal civilian information systems to
5 the Center;

6 “(B) provide cyber incident detection, anal-
7 ysis, mitigation, and response information to
8 the Center; and

9 “(C) immediately send and disclose cyber
10 threat information received by a cyber security
11 provider to the Center; and

12 “(10) perform such other duties as the Sec-
13 retary may require relating to the coordination of
14 the national protection of, prevention, mitigation of,
15 and recovery from cyber incidents.

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

19 “(1) analyze and integrate all information re-
20 ceived from other Federal agencies, State and local
21 governments, private entities, and the critical infra-
22 structure sectors, and share such cyber threat infor-
23 mation and analysis in near real-time;

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

1 share actionable assessments of critical infrastruc-
2 ture sector risks from cyber incidents and to assist
3 critical infrastructure sectors in making continuous
4 improvements to the security and resiliency of the
5 Nation’s critical infrastructure;

6 “(3) facilitate cross sector integration, identi-
7 fication, and analysis of key interdependencies to
8 prevent related and consequential impacts to other
9 critical infrastructure sectors; and

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

14 “(f) INFORMATION SHARING PROCEDURES AND PRO-
15 TECTIONS.—

16 “(1) IN GENERAL.—The Center may enter into
17 an information sharing relationship with any private
18 entity for the sharing of cyber threat information for
19 cybersecurity purposes in accordance with this sub-
20 section.

21 “(2) AGREEMENTS.—

22 “(A) CENTER MEMORANDUM OF UNDER-
23 STANDING.—To enter into an information shar-
24 ing relationship with the Center under this sub-
25 section, a private entity shall enter into a

1 memorandum of understanding with the Center
2 that sets forth the general terms of the rela-
3 tionship, including all information protections
4 and liability exemptions as set forth in this sub-
5 section. A memorandum of understanding de-
6 scribed in this paragraph shall be finalized
7 within 72 hours of a request to enter into an
8 information sharing relationship with the Cen-
9 ter. The Center Memorandum of Understanding
10 shall be the only agreement required to enter
11 into a formal information sharing relationship
12 with the Center. Any information sharing con-
13 tractual agreement in effect prior to the date of
14 the enactment of this paragraph is exempt from
15 this paragraph.

16 “(B) OTHER AGREEMENTS.—Nothing in
17 this paragraph shall preclude the Department
18 or the Center from entering into other informa-
19 tion sharing agreements with private entities.
20 All such other agreements shall include all in-
21 formation protections and liability exemptions
22 as set forth in this section and must be nego-
23 tiated and finalized within 60 days of a request
24 to enter into an agreement.

25 “(3) INFORMATION SHARING.—

1 “(A) PRIVATE ENTITIES.—Notwith-
2 standing any other provision of law, a private
3 entity may, for cybersecurity purposes, share
4 cyber threat information obtained on its own in-
5 formation system as provided in this subsection.

6 “(B) CYBERSECURITY PROVIDERS.—Not-
7 withstanding any other provision of law, a cy-
8 bersecurity provider may, with the express con-
9 sent of a protected private entity for which such
10 cybersecurity provider is providing goods or
11 services for cybersecurity purposes, use cyberse-
12 curity systems to identify and obtain cyber
13 threat information to protect the rights and
14 property of such protected private entity.

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

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

24 “(4) PRIVACY PROTECTIONS FOR INFORMATION
25 SHARING.—

1 “(A) POLICIES AND PROCEDURES.—The
2 Office of Privacy of the Department on an on-
3 going basis shall—

4 “(i) review all policies and procedures
5 governing the sharing of cyber threat in-
6 formation by a private entity with the Cen-
7 ter, or by a private entity with another pri-
8 vate entity through an official Information
9 Sharing and Analysis Center, to ensure
10 that such policies and procedures are con-
11 sistent with the Fair Information Practice
12 Principles.; and

13 “(ii) prepare, as necessary, privacy
14 impact assessments to ensure all relevant
15 constitutional, legal, and privacy protec-
16 tions are being followed.

17 “(B) OFFICE OF PRIVACY REPORT.—The
18 Office of Privacy of the Department shall pre-
19 pare an annual report to Congress containing
20 an assessment of the effectiveness of the pri-
21 vacy measures governing the sharing of cyber
22 threat information through the Center and the
23 official Information Sharing and Analysis Cen-
24 ters. Such report shall be made available upon
25 request to the Committee on Homeland Secu-

1 rity of the House of Representatives and the
2 Committee on Homeland Security and Govern-
3 mental Affairs of the Senate.

4 “(5) PROTECTION OF INFORMATION.—

5 “(A) IN GENERAL.—Any cyber threat in-
6 formation shared under this section shall be
7 used solely for cybersecurity purposes and shall
8 only be further disclosed to any official Infor-
9 mation Sharing and Analysis Center or as oth-
10 erwise expressly agreed to by the Secretary.

11 “(B) UNFAIR PRACTICES AND ANTITRUST
12 EXEMPTION.—Cyber threat information shared
13 in accordance with this section—

14 “(i) may not be used by a private en-
15 tity to gain an unfair competitive advan-
16 tage to the detriment of a private entity
17 that shared information through the Cen-
18 ter or otherwise under this section; and

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

1 “(C) FEDERAL GOVERNMENT.—Informa-
2 tion shared with the Federal Government
3 through the Center or otherwise under this sec-
4 tion—

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

7 “(ii) shall be considered proprietary
8 information and may not be disclosed to an
9 entity outside the Federal Government un-
10 less otherwise expressly authorized by the
11 private entity sharing such information;

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

14 “(iv) shall be exempt from disclosure
15 under a State, local, or tribal law or regu-
16 lation that requires public disclosure of in-
17 formation by a public or quasi-public enti-
18 ty.

19 “(6) FEDERAL PREEMPTION.—This section
20 supercedes any law of a State or political subdivision
21 of a State that restricts or otherwise expressly regu-
22 lates the sharing of information by a private entity
23 as provided in this section.

24 “(7) LIABILITY EXEMPTION.—

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

5 “(i) using cybersecurity systems to
6 identify or obtain cyber threat information
7 or for sharing such information in accord-
8 ance with this section; or

9 “(ii) decisions made for cybersecurity
10 purposes and based on cyber threat infor-
11 mation or for sharing such information in
12 accordance with this section.

13 “(B) LACK OF GOOD FAITH.—For pur-
14 poses of the exemption from liability under sub-
15 paragraph (A), a lack of good faith includes
16 any act or omission taken with intent to injure,
17 defraud, or otherwise endanger any individual
18 government entity or private entity.

19 “(C) APPLICABILITY.—This section shall
20 apply to information shared by a private entity
21 to the Center or a private entity to another pri-
22 vate entity through an official Information
23 Sharing and Analysis Center.

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

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

3 “(9) DEPARTMENT USE OF INFORMATION.—

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

8 “(B) DEPARTMENTAL CAUSE OF AC-
9 TION.—If the Secretary intentionally violates
10 any of the restrictions on the disclosure, use, or
11 protection of information shared by a private
12 entity with the Center in accordance with this
13 section, a cause of action may lie or be main-
14 tained by a person in a Federal court.

15 “(g) SEE SOMETHING, SAY SOMETHING FOR CYBER
16 THREATS.—

17 “(1) IN GENERAL.—The Secretary shall estab-
18 lish policies and procedures at the Center to encour-
19 age and facilitate any private entity or individual,
20 whether or not they have an information sharing re-
21 lationship with the Center, to report any type of in-
22 formation that may pertain to a cyber threat to crit-
23 ical infrastructure. To the extent practicable, any
24 person should make a good faith effort to share any
25 information that concerns—

1 “(A) the extent and likelihood of death, in-
2 jury, or serious adverse effects to human health
3 and safety caused by a disruption, destruction,
4 or unauthorized use of critical infrastructure;

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

8 “(C) harm to the economy that would re-
9 sult from the disruption, destruction, or unau-
10 thorized use of critical infrastructure.

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

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

17 “(h) ACQUISITION AUTHORITIES.—

18 “(1) IN GENERAL.—The Center is authorized to
19 use the authorities under subsections (c)(1) and
20 (d)(1)(B) of section 2304 of title 10, United States
21 Code, instead of the authorities under subsections
22 (a)(1) and (b)(2) of section 3304 of title 41, United
23 States Code, subject to all other requirements of sec-
24 tions 3301 and 3304 of title 41, United States Code.

1 “(2) GUIDELINES.—Not later than 90 days
2 after the date of the enactment of this section, the
3 chief procurement officer of the Department shall
4 issue guidelines for use of the authority under para-
5 graph (1).

6 “(3) ANNUAL REPORT.—Not later than 60 days
7 after the last day of a fiscal year, the Secretary shall
8 submit to the Committee on Homeland Security of
9 the House of Representatives and the Committee on
10 Homeland Security of the Senate a report on the use
11 of the authority under paragraph (1) during that fis-
12 cal year. Each such report shall contain—

13 “(A) the number of contract actions taken
14 under the authority under such paragraph dur-
15 ing the period covered by the report; and

16 “(B) for each such contract action—

17 “(i) the total dollar value of the con-
18 tract action;

19 “(ii) a summary of the market re-
20 search conducted by the Center, including
21 a list of all offerors who were considered
22 and those who actually submitted bids, in
23 order to determine that use of the author-
24 ity was appropriate; and

1 “(iii) a copy of the justification and
2 approval documents required by section
3 3304(e) of title 41, United States Code.

4 “(i) REPORT OF CYBER ATTACKS AGAINST GOVERN-
5 MENT NETWORKS.—The Secretary shall submit to the
6 Committee on Homeland Security of the House of Rep-
7 resentatives and the Committee on Homeland Security
8 and Governmental Affairs of the Senate an annual report
9 that summarizes major cyber incidents involving Federal
10 civilian agency information systems and provides aggre-
11 gate statistics on the number of breaches, the volume of
12 data exfiltrated, the consequential impact, and the esti-
13 mated cost of remedying the breaches involving Federal
14 civilian information systems. The contents of the report
15 may be provided to Congress through real-time electronic
16 dashboard reporting in lieu of a written document.

17 “(j) REPORT ON THE OPERATIONS OF THE CEN-
18 TER.—The Secretary, in consultation with the Sector Co-
19 ordinating Councils and appropriate Federal Government
20 entities, shall submit to the Committee on Homeland Se-
21 curity of the House of Representatives and the Committee
22 on Homeland Security and Governmental Affairs of the
23 Senate an annual report on the capability and capacity
24 of the Center to carry out its cybersecurity mission in ac-
25 cordance with this Act.

1 “(k) FUNDING.—Of the amounts authorized to be ap-
2 propriated for each of fiscal years 2014, 2015, and 2016,
3 for the Cybersecurity and Communications Office of the
4 Department, the Secretary is authorized to use not less
5 than \$25,000,000 for any such year to ensure the partici-
6 pation of all official sector Information Sharing and Anal-
7 ysis Centers in the Center.”.

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

 “227. National Cybersecurity and Communications Integration Center.”.

12 (c) GAO REPORT.—Not later than one year after the
13 date of the enactment of this Act, the Comptroller General
14 of the United States shall submit to the Committee on
15 Homeland Security of the House of Representatives and
16 the Committee on Homeland Security of the Senate a re-
17 port on the effectiveness of the National Cybersecurity and
18 Communications Integration Center established under sec-
19 tion 227 of the Homeland Security Act of 2002, as added
20 by subsection (a) to carry out it’s cybersecurity mission
21 in accordance with this Act.

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

23 (a) IN GENERAL.—Subtitle C of title II of the Home-
24 land Security Act of 2002, as amended by sections 202

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

3 **“SEC. 228. CYBER INCIDENT RESPONSE TEAMS.**

4 “The Secretary shall—

5 “(1) Provide timely technical assistance and cri-
6 sis management to Federal, State, and local govern-
7 ment entities, and private entities from cyber inci-
8 dents affecting critical infrastructure;

9 “(2) Provide actionable recommendations on se-
10 curity and resilience measures and countermeasures
11 to Federal, State, and local government entities, pri-
12 vate entities, and the critical infrastructure sectors
13 prior to, during, and after a cyber incident.

14 “(3) Develop a national cybersecurity incident
15 response plan which shall—

16 “(A) coordinate with the Sector Coordi-
17 nating Councils, Federal, State, and local gov-
18 ernments, and other relevant entities to annu-
19 ally develop, implement, and exercise the Na-
20 tional Cybersecurity Incident Response Plan
21 that details the roles and responsibilities of crit-
22 ical infrastructure owners, critical infrastruc-
23 ture operators, and Federal, State, and local
24 governments to protect from, prevent, mitigate,
25 respond to, and recover from cyber incidents;

1 “(B) ensure the National Cybersecurity In-
2 cident Response Plan is flexible enough to re-
3 flect a changing cyber threat environment and
4 incorporate best practices and lessons learned
5 from regular exercises, training, and after-ac-
6 tion reports.”.

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

 “228. Cyber incident response teams.”.

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

12 (a) IN GENERAL.—Subtitle C of title II of the Home-
13 land Security Act of 2002, as amended by sections 202,
14 203, and 204, is further amended by adding at the end
15 the following new section:

16 **“SEC. 229. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

17 “(a) ASSESSMENT.—The Secretary shall regularly
18 assess the readiness and capacity of the workforce of the
19 Department to meet the needs of the cybersecurity mission
20 of the Department.

21 “(b) STRATEGY REQUIRED.—Not later than 180
22 days after the date of the enactment of this section, the
23 Secretary shall develop and maintain a comprehensive
24 workforce strategy designed to enhance the readiness, ca-
25 pacity, training, recruitment, and retention of the cyberse-

1 curity personnel of the Department. Such strategy shall
2 include a five-year plan on recruitment of personnel for
3 the workforce of the Department and ten-year projections
4 of the workforce needs of the Department.

5 “(c) UPDATES.—The Secretary shall update the
6 strategy maintained under subsection (b) as necessary.”.

7 (b) CLERICAL AMENDMENT.—The table of contents
8 in section 1(b) of such Act, as amended by sections 202,
9 203, and 204, is further amended by adding at the end
10 the following new item:

“229. Assessment of cybersecurity workforce.”.

11 **SEC. 207. PERSONNEL AUTHORITIES.**

12 (a) IN GENERAL.—Subtitle C of title II of the Home-
13 land Security Act of 2002, as amended by sections 202,
14 203, 204, 205, and 206 is further amended by adding at
15 the end the following new section:

16 **“SEC. 229A. PERSONNEL AUTHORITIES.**

17 “(a) IN GENERAL.—In order to assure that the De-
18 partment has the necessary resources to carry out the mis-
19 sion of securing Federal civilian information systems and
20 critical infrastructure information systems, the Secretary
21 may, as necessary, convert competitive service positions,
22 and the incumbents of such positions, within the Office
23 of Cybersecurity and Communications to excepted service
24 positions, or may establish new positions within the Office
25 of Cybersecurity and Communications in the excepted

1 service, to the extent that the Secretary determines such
2 positions are necessary to carry out the cybersecurity
3 functions of the Department.

4 “(b) COMPENSATION.—The Secretary may—

5 “(1) fix the compensation of individuals who
6 serve in positions referred to in subsection (a) in re-
7 lation to the rates of pay provided for comparable
8 positions in the Department and subject to the same
9 limitations on maximum rates of pay established for
10 employees of the Department by law or regulations;
11 and

12 “(2) provide additional forms of compensation,
13 including benefits, incentives, and allowances that
14 are consistent with and not in excess of the level au-
15 thorized for comparable positions authorized under
16 title 5, United States Code.

17 “(c) RETENTION BONUSES.—Notwithstanding any
18 other provision of law, the Secretary may pay a retention
19 bonus to any employee appointed under this section, if the
20 Secretary determines that the bonus is needed to retain
21 essential personnel. Before announcing the payment of a
22 bonus under this subsection, the Secretary shall submit
23 a written explanation of such determination to the Com-
24 mittee on Homeland Security of the House of Representa-

1 tives and the Committee on Homeland Security and Gov-
2 ernmental Affairs of the Senate.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of such Act, as amended by sections 202,
5 203, and 204, is further amended by adding at the end
6 the following new item:

“229A. Personnel authorities.”.

7 **SEC. 208. STREAMLINING OF DEPARTMENT CYBERSECU-**
8 **RITY ORGANIZATION.**

9 (a) CYBERSECURITY AND INFRASTRUCTURE PRO-
10 TECTION DIRECTORATE.—The National Protection and
11 Programs Directorate of the Department of Homeland Se-
12 curity shall after the date of the enactment of this Act
13 be known and designated as the “Cybersecurity and Infra-
14 structure Protection Directorate”. Any reference to such
15 Directorate in any law, regulation, map, document, record,
16 or other paper of the United States shall be considered
17 to be a reference to the Cybersecurity and Infrastructure
18 Protection Directorate.

19 (b) SENIOR LEADERSHIP OF CYBERSECURITY AND
20 INFRASTRUCTURE PROTECTION DIRECTORATE.—After
21 the date of the enactment of this Act, there shall be no
22 more than three senior leadership positions in the Cyberse-
23 curity and Infrastructure Protection Directorate, includ-
24 ing one Under Secretary.

1 (c) REPORT TO CONGRESS.—To improve the oper-
2 ational capability and effectiveness in carrying out the cy-
3 bersecurity mission of the Department, the Secretary of
4 Homeland Security shall submit to Congress a report on—

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

8 (2) recommendations for restructuring the
9 SAFETY Act office within the Department to ele-
10 vate the profile and mission of the office. The report
11 shall also provide an analysis on the feasibility of
12 utilizing third-party registrars for improving the
13 throughput and effectiveness of the certification
14 process.

15 **TITLE III—INDUSTRY-LED INI-**
16 **TIATIVES TO ADDRESS**
17 **VULNERABILITIES AND GAPS**
18 **IN CYBERSECURITY**

19 **SEC. 301. INDUSTRY-LED INITIATIVES TO ADDRESS**
20 **VULNERABILITIES AND GAPS IN CYBERSECU-**
21 **RITY.**

22 (a) IN GENERAL.—Subtitle C of title II of the Home-
23 land Security Act of 2002, as amended by sections 202,
24 203, 204, 205, 206, and 207 is further amended by adding
25 at the end the following new section:

1 **“SEC. 229B. INDUSTRY-LED INITIATIVES TO ADDRESS**
2 **VULNERABILITIES IN CYBERSECURITY.**

3 “(a) INDUSTRY LED INITIATIVES TO ESTABLISH CY-
4 BERSECURITY GUIDELINES.—The Sector Coordinating
5 Council for each critical infrastructure sector established
6 under section 226 shall meet no less than six times per
7 year to continually address vulnerabilities and gaps in cy-
8 bersecurity across the relevant sector. Such meetings shall
9 be conducted to—

10 “(1) assess, on an ongoing basis, the state of
11 cybersecurity for the relevant critical infrastructure
12 sector to determine guidelines for the critical infra-
13 structure sector, taking into consideration cyber
14 threats, vulnerabilities, and risks, including—

15 “(A) the actual or assessed threat, includ-
16 ing a consideration of adversary capability and
17 intent, preparedness, target attractiveness and
18 deterrence capabilities;

19 “(B) the extent and likelihood of death, in-
20 jury, or serious adverse effects to human health
21 and safety caused by a disruption, destruction,
22 or unauthorized use of critical infrastructure;

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

1 “(D) the harm to the economy that would
2 result from the disruption, destruction or unau-
3 thorized use of critical infrastructure;

4 “(2) develop guidelines to mitigate cyber risks
5 for the critical infrastructure sector, taking into con-
6 sideration—

7 “(A) current Federal and State regula-
8 tions, risk management determinations, recog-
9 nized industry and relevant government best
10 practices and any other relevant information to
11 enhance and address vulnerabilities and gaps in
12 cybersecurity for the critical infrastructure sec-
13 tor;

14 “(B) consultations with cybersecurity ex-
15 perts and institutions;

16 “(C) development of cybersecurity guide-
17 lines tailored to the size and scope of an entity
18 within a sector;

19 “(D) neutrality of technology; and

20 “(E) harmonization with international
21 standards to the greatest extent practicable;

22 “(3) determine, on an ongoing basis, whether
23 enhancements to cybersecurity guidelines are nec-
24 essary, and if so, ensure flexibility to reflect a
25 changing cyber threat environment; and

1 “(4) encourage private entities within the crit-
2 ical infrastructure sector to voluntarily adopt cyber-
3 security guidelines developed by the Sector Co-
4 ordinating Council for a critical infrastructure sec-
5 tor.

6 “(b) INDUSTRY-LED ENFORCEMENT OF GUIDE-
7 LINES.—

8 “(1) IN GENERAL.—The Sector Coordinating
9 Councils shall coordinate efforts across the sector to
10 encourage the industry-led enforcement by the sector
11 of voluntarily adopted cybersecurity guidelines to en-
12 sure the mitigation of risks for cybersecurity and the
13 hardening of critical infrastructure sector wide.

14 “(2) THIRD PARTY TECHNICAL ASSISTANCE
15 AND VOLUNTARY ASSESSMENTS.—The Sector Co-
16 ordinating Councils may enter into agreements with
17 qualified third party private entities to—

18 “(A) provide technical assistance to private
19 entities that seek assistance in adopting the cy-
20 bersecurity guidelines established by the Sector
21 Coordinating Council; and

22 “(B) conduct assessments to assess wheth-
23 er a private entity which has voluntarily adopt-
24 ed cybersecurity guidelines is meeting the cy-

1 bersecurity guidelines established by the Sector
2 Coordinating Council.

3 “(c) QUARTERLY COLLABORATION MEETINGS.—The
4 Sector Coordinating Council for each critical infrastruc-
5 ture sector shall meet with the Department on a quarterly
6 basis to—

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

10 “(2) discuss the state of cybersecurity for the
11 critical infrastructure sector, taking into consider-
12 ation cyber threats, vulnerabilities, and risks;

13 “(3) discuss the Department’s efforts to protect
14 critical infrastructure as set forth in section 226;

15 “(4) afford the Secretary an opportunity to un-
16 derstand the cybersecurity guidelines established by
17 the Sector Coordinating Council to address
18 vulnerabilities and gaps in cybersecurity;

19 “(5) discuss efforts being taken by the critical
20 infrastructure sector to encourage and enforce the
21 voluntary adoption of cybersecurity guidelines estab-
22 lished by the Sector Coordinating Council across the
23 sector; and

24 “(6) share information and ideas to ensure
25 greater cybersecurity for the sector.

1 “(d) REPORT TO CONGRESS.—

2 “(1) IN GENERAL.—The Secretary shall submit
3 to the Committee on Homeland Security of the
4 House of Representatives and the Committee on
5 Homeland Security and Governmental Affairs of the
6 Senate an annual report on the state of cybersecu-
7 rity for each critical infrastructure sector based on
8 discussions between the Department and the Sector
9 Coordinating Council from the quarterly collabora-
10 tions meeting under subsection (c). The Secretary
11 shall maintain a copy of the report on the Internet
12 website of the Department.

13 “(2) SECTOR COORDINATING COUNCIL RE-
14 SPONSE.—Before making public and submitting the
15 report to the Committees under paragraph (1), the
16 Secretary shall provide a draft of the report to the
17 Sector Coordinating Council for the critical infra-
18 structure sector covered by the report. The Sector
19 Coordinating Council shall provide to the Secretary
20 a written response to the report within 45 days of
21 receiving the draft. The Secretary shall include the
22 written response of the Sector Coordinating Council
23 in the final report submitted under paragraph (1).

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

1 Federal Government regulatory authority, or permit the
2 Federal Government to adopt the cybersecurity guidelines
3 established by a Sector Coordinating Council for regu-
4 latory purposes.”.

5 (b) CLERICAL AMENDMENT.—The table of contents
6 in section 1(b) of such Act, as amended by sections 202,
7 203, 204, 205, and 206 is further amended by adding at
8 the end the following new item:

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

9 **SEC. 302. SAFETY ACT AND SIGNIFICANT CYBER INCI-**
10 **DENTS.**

11 (a) IN GENERAL.—The Support Anti-Terrorism By
12 Fostering Effective Technologies Act of 2002 (6 U.S.C.
13 441 et seq.) is amended—

14 (1) in section 862—

15 (A) in the heading for subsection (b), by
16 striking “DESIGNATION OF QUALIFIED ANTI-
17 TERRORISM TECHNOLOGIES” and inserting
18 “DESIGNATION OF ANTI-TERRORISM AND CY-
19 BERSECURITY TECHNOLOGIES”;

20 (B) in subsection (b) in paragraphs (3),
21 (4), and (5), by striking “anti-terrorism” each
22 place that such appears and inserting “anti-ter-
23 rorism or cybersecurity”;

24 (C) in paragraph (7)—

1 (i) by inserting “or cybersecurity tech-
2 nology” after “Anti-terrorism technology”;
3 and

4 (ii) by inserting “or significant cyber
5 incidents” after “acts of terrorism”;

6 (2) in section 863 (6 U.S.C. 442)—

7 (A) by striking “anti-terrorism” each place
8 that such appears and inserting “anti-terrorism
9 or cybersecurity”;

10 (B) by striking “act of terrorism” each
11 place that such appears and inserting “act of
12 terrorism or significant cyber incident”;

13 (C) by striking “acts of terrorism” each
14 place that such appears and inserting “acts of
15 terrorism or significant cyber incidents”;

16 (3) in section 864 (6 U.S.C. 443)—

17 (A) by striking “anti-terrorism” each place
18 that such appears and inserting “anti-terrorism
19 or cybersecurity”;

20 (B) by striking “act of terrorism” each
21 place that such appears and inserting “act of
22 terrorism or significant cyber incident”;

23 (4) in section 865 (6 U.S.C. 444)—

24 (A) in paragraph (1) by inserting “or cy-
25 bersecurity” after “anti-terrorism”;

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

3 “(7) SIGNIFICANT CYBER INCIDENT.—

4 “(A) IN GENERAL.—The term ‘significant
5 cyber incident’ means any act that the Sec-
6 retary determines meets the requirements under
7 subparagraph (B), as such requirements are
8 further defined and specified by the Secretary.

9 “(B) REQUIREMENTS.—A significant cyber
10 incident meets the requirements of this sub-
11 paragraph if the attack—

12 “(i) is unlawful, unauthorized, or oth-
13 erwise exceeds authorized access authority;

14 “(ii)(I) attempts to or actually dis-
15 rupts or imminently jeopardizes the integ-
16 rity, operation, confidentiality, or avail-
17 ability of programmable electronic devices,
18 communication networks including hard-
19 ware, software and data that are essential
20 to their reliable operation, electronic stor-
21 age device, or any other electronic informa-
22 tion system or the information that system
23 controls, processes, stores, or transmits
24 electronic information, including for any
25 information system or component thereof

1 used to operate covered critical infrastruc-
2 ture; or

3 “(II) results in the theft or misapprop-
4 priation in electronic or printed form of
5 private or government information, intel-
6 lectual property, or personally identifiable
7 information; and

8 “(iii) causes material harm or results
9 in material economic loss to a person,
10 property, or entity, in or outside the
11 United States.

12 “(8) COVERED CRITICAL INFRASTRUCTURE.—
13 In this section, the term ‘covered critical infrastruc-
14 ture’ means any facility or function that, by way of
15 cyber vulnerability, the destruction or disruption of
16 or unauthorized access to could result in—

17 “(A) a significant loss of life;

18 “(B) a major economic disruption, includ-
19 ing—

20 “(i) the immediate failure of, or loss
21 of confidence in, a major financial market;
22 or

23 “(ii) the sustained disruption of finan-
24 cial systems that would lead to long term

1 catastrophic economic damage to the
2 United States;

3 “(C) mass evacuations of a major popu-
4 lation center for an extended length of time; or

5 “(D) severe degradation of national secu-
6 rity or national security capabilities, including
7 intelligence and defense functions, but excluding
8 military facilities.”.

9 (b) FUNDING.—Of the amounts authorized to be ap-
10 propriated for each of fiscal years 2014, 2015, and 2016
11 for the Science and Technology Directorate, the Secretary
12 is authorized to use not less than \$20,000,000 for any
13 such year for the Department’s SAFETY Act office.