

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 3696
OFFERED BY MR. McCAUL OF TEXAS**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “National Cybersecurity
3 and Critical Infrastructure Protection Act of 2014”.

4 SEC. 2. TABLE OF CONTENTS.

5 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. Homeland Security Act of 2002 definitions.
- Sec. 102. Enhancement of cybersecurity.
- Sec. 103. Protection of critical infrastructure and information sharing.
- Sec. 104. National Cybersecurity and Communications Integration Center.
- Sec. 105. Cyber incident response and technical assistance.
- Sec. 106. Streamlining of Department cybersecurity organization.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

- Sec. 201. Public-private collaboration on cybersecurity.
- Sec. 202. SAFETY Act and qualifying cyber incidents.
- Sec. 203. Prohibition on new regulatory authority.
- Sec. 204. Prohibition on additional authorization of appropriations.
- Sec. 205. Prohibition on collection activities to track individuals’ personally identifiable information.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

- Sec. 301. Homeland security cybersecurity workforce.
- Sec. 302. Personnel authorities.

1 **TITLE I—SECURING THE NATION**
2 **AGAINST CYBER ATTACK**

3 **SEC. 101. HOMELAND SECURITY ACT OF 2002 DEFINITIONS.**

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

7 “(19) The term ‘critical infrastructure’ has the
8 meaning given that term in section 1016(e) of the
9 USA Patriot Act (42 U.S.C. 5195c(e)).

10 “(20) The term ‘critical infrastructure owner’
11 means a person that owns critical infrastructure.

12 “(21) The term ‘critical infrastructure operator’
13 means a critical infrastructure owner or other per-
14 son that manages, runs, or operates, in whole or in
15 part, the day-to-day operations of critical infrastruc-
16 ture.

17 “(22) The term ‘cyber incident’ means an inci-
18 dent, or an attempt to cause an incident, that, if
19 successful, would—

20 “(A) jeopardize or imminently jeopardize,
21 without lawful authority, the security, integrity,
22 confidentiality, or availability of an information
23 system or network of information systems or
24 any information stored on, processed on, or
25 transiting such a system or network;

1 “(B) constitute a violation or imminent
2 threat of violation of law, security policies, secu-
3 rity procedures, or acceptable use policies re-
4 lated to such a system or network, or an act of
5 terrorism against such a system or network; or

6 “(C) result in the denial of access to or
7 degradation, disruption, or destruction of such
8 a system or network, or the defeat of an oper-
9 ations control or technical control essential to
10 the security or operation of such a system or
11 network.

12 “(23) The term ‘cybersecurity mission’ means
13 activities that encompass the full range of threat re-
14 duction, vulnerability reduction, deterrence, incident
15 response, resiliency, and recovery activities to foster
16 the security and stability of cyberspace.

17 “(24) The term ‘cybersecurity purpose’ means
18 the purpose of ensuring the security, integrity, con-
19 fidentiality, or availability of, or safeguarding, an in-
20 formation system or network of information systems,
21 including protecting such a system or network, or
22 data residing on such a system or network, including
23 protection of such a system or network, from—

24 “(A) a vulnerability of such a system or
25 network;

1 “(B) a threat to the security, integrity,
2 confidentiality, or availability of such a system
3 or network, or any information stored on, proc-
4 essed on, or transiting such a system or net-
5 work;

6 “(C) efforts to deny access to or degrade,
7 disrupt, or destroy such a system or network; or

8 “(D) efforts to gain unauthorized access to
9 such a system or network, including to gain
10 such unauthorized access for the purpose of
11 exfiltrating information stored on, processed on,
12 or transiting such a system or network.

13 “(25) The term ‘cyber threat’ means any action
14 that may result in unauthorized access to,
15 exfiltration of, manipulation of, harm of, or impair-
16 ment to the security, integrity, confidentiality, or
17 availability of an information system or network of
18 information systems, or information that is stored
19 on, processed by, or transiting such a system or net-
20 work.

21 “(26) The term ‘cyber threat information’
22 means information directly pertaining to—

23 “(A) a vulnerability of an information sys-
24 tem or network of information systems of a
25 government or private entity;

1 “(B) a threat to the security, integrity,
2 confidentiality, or availability of such a system
3 or network of a government or private entity, or
4 any information stored on, processed on, or
5 transiting such a system or network;

6 “(C) efforts to deny access to or degrade,
7 disrupt, or destroy such a system or network of
8 a government or private entity;

9 “(D) efforts to gain unauthorized access to
10 such a system or network, including to gain
11 such unauthorized access for the purpose of
12 exfiltrating information stored on, processed on,
13 or transiting such a system or network; or

14 “(E) an act of terrorism against an infor-
15 mation system or network of information sys-
16 tems.

17 “(27) The term ‘Federal civilian information
18 systems’—

19 “(A) means information, information sys-
20 tems, and networks of information systems that
21 are owned, operated, controlled, or licensed for
22 use by, or on behalf of, any Federal agency, in-
23 cluding such systems or networks used or oper-
24 ated by another entity on behalf of a Federal
25 agency; but

1 “(B) does not include—

2 “(i) a national security system; or

3 “(ii) information, information sys-
4 tems, and networks of information systems
5 that are owned, operated, controlled, or li-
6 censed solely for use by, or on behalf of,
7 the Department of Defense, a military de-
8 partment, or an element of the intelligence
9 community.

10 “(28) The term ‘information security’ means
11 the protection of information, information systems,
12 and networks of information systems from unauthor-
13 ized access, use, disclosure, disruption, modification,
14 or destruction in order to provide—

15 “(A) integrity, including guarding against
16 improper information modification or destruc-
17 tion, including ensuring nonrepudiation and au-
18 thenticity;

19 “(B) confidentiality, including preserving
20 authorized restrictions on access and disclosure,
21 including means for protecting personal privacy
22 and proprietary information; and

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

1 “(29) The term ‘information system’ means the
2 underlying framework and functions used to process,
3 transmit, receive, or store information electronically,
4 including programmable electronic devices, commu-
5 nications networks, and industrial or supervisory
6 control systems and any associated hardware, soft-
7 ware, or data.

8 “(30) The term ‘private entity’ means any indi-
9 vidual or any private or publically-traded company,
10 public or private utility (including a utility that is a
11 unit of a State or local government, or a political
12 subdivision of a State government), organization, or
13 corporation, including an officer, employee, or agent
14 thereof.

15 “(31) The term ‘shared situational awareness’
16 means an environment in which cyber threat infor-
17 mation is shared in real time between all designated
18 Federal cyber operations centers to provide action-
19 able information about all known cyber threats.”.

20 **SEC. 102. ENHANCEMENT OF CYBERSECURITY.**

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

1 **“SEC. 226. ENHANCEMENT OF CYBERSECURITY.**

2 “The Secretary, in collaboration with the heads of
3 other appropriate Federal Government entities, shall con-
4 duct activities for cybersecurity purposes, including the
5 provision of shared situational awareness to each other to
6 enable real-time, integrated, and operational actions to
7 protect from, prevent, mitigate, respond to, and recover
8 from cyber incidents.”.

9 (b) CLERICAL AMENDMENTS.—

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

13 **“Subtitle C—Cybersecurity and**
14 **Information Sharing”.**

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

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

“Sec. 226. Enhancement of cybersecurity.”;

19 and

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

“Subtitle C—Cybersecurity and Information Sharing”.

1 **SEC. 103. 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, as amended by section 102,
5 is further amended by adding at the end the following new
6 section:

7 **“SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE**
8 **AND INFORMATION SHARING.**

9 “(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

10 “(1) IN GENERAL.—The Secretary shall coordi-
11 nate, on an ongoing basis, with Federal, State, and
12 local governments, critical infrastructure owners,
13 critical infrastructure operators, and other cross sec-
14 tor coordinating entities to—

15 “(A) facilitate a national effort to
16 strengthen and maintain secure, functioning,
17 and resilient critical infrastructure from cyber
18 threats;

19 “(B) ensure that Department policies and
20 procedures enable critical infrastructure owners
21 and critical infrastructure operators to receive
22 real-time, actionable, and relevant cyber threat
23 information;

24 “(C) seek industry sector-specific expertise
25 to—

1 “(i) assist in the development of vol-
2 untary security and resiliency strategies;
3 and

4 “(ii) ensure that the allocation of Fed-
5 eral resources are cost effective and reduce
6 any burden on critical infrastructure own-
7 ers and critical infrastructure operators;

8 “(D) upon request of entities, facilitate
9 and assist risk management efforts of such en-
10 tities to reduce vulnerabilities, identify and dis-
11 rupt threats, and minimize consequences to
12 their critical infrastructure;

13 “(E) upon request of critical infrastructure
14 owners or critical infrastructure operators, pro-
15 vide education and assistance to such owners
16 and operators on how they may use protective
17 measures and countermeasures to strengthen
18 the security and resilience of the Nation’s crit-
19 ical infrastructure; and

20 “(F) coordinate a research and develop-
21 ment strategy to facilitate and promote ad-
22 vancements and innovation in cybersecurity
23 technologies to protect critical infrastructure.

24 “(2) ADDITIONAL RESPONSIBILITIES.—The
25 Secretary shall—

1 “(A) manage Federal efforts to secure,
2 protect, and ensure the resiliency of Federal ci-
3 vilian information systems, and, upon request of
4 critical infrastructure owners or critical infra-
5 structure operators, support such owners’ and
6 operators’ efforts to secure, protect, and ensure
7 the resiliency of critical infrastructure from
8 cyber threats;

9 “(B) direct an entity within the Depart-
10 ment to serve as a Federal civilian entity by
11 and among Federal, State, and local govern-
12 ments, private entities, and critical infrastruc-
13 ture sectors to provide multi-directional sharing
14 of real-time, actionable, and relevant cyber
15 threat information;

16 “(C) build upon existing mechanisms to
17 promote a national awareness effort to educate
18 the general public on the importance of secur-
19 ing information systems;

20 “(D) upon request of Federal, State, and
21 local government entities and private entities,
22 facilitate expeditious cyber incident response
23 and recovery assistance, and provide analysis
24 and warnings related to threats to and
25 vulnerabilities of critical information systems,

1 crisis and consequence management support,
2 and other remote or on-site technical assistance
3 with the heads of other appropriate Federal
4 agencies to Federal, State, and local govern-
5 ment entities and private entities for cyber inci-
6 dents affecting critical infrastructure; and

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

12 “(3) RULE OF CONSTRUCTION.—Nothing in
13 this section may be construed to require any private
14 entity to request assistance from the Secretary, or
15 require any private entity requesting such assistance
16 to implement any measure or recommendation sug-
17 gested by the Secretary.

18 “(b) CRITICAL INFRASTRUCTURE SECTORS.—The
19 Secretary, in collaboration with the heads of other appro-
20 priate Federal agencies, shall designate critical infrastruc-
21 ture sectors (that may include subdivisions of sectors with-
22 in a sector as the Secretary may determine appropriate).
23 The critical infrastructure sectors designated under this
24 subsection may include the following:

25 “(1) Chemical.

- 1 “(2) Commercial facilities.
- 2 “(3) Communications.
- 3 “(4) Critical manufacturing.
- 4 “(5) Dams.
- 5 “(6) Defense Industrial Base.
- 6 “(7) Emergency services.
- 7 “(8) Energy.
- 8 “(9) Financial services.
- 9 “(10) Food and agriculture.
- 10 “(11) Government facilities.
- 11 “(12) Healthcare and public health.
- 12 “(13) Information technology.
- 13 “(14) Nuclear reactors, materials, and waste.
- 14 “(15) Transportation systems.
- 15 “(16) Water and wastewater systems.
- 16 “(17) Such other sectors as the Secretary de-
- 17 termines appropriate.
- 18 “(c) SECTOR SPECIFIC AGENCIES.—The Secretary,
- 19 in collaboration with the relevant critical infrastructure
- 20 sector and the heads of other appropriate Federal agen-
- 21 cies, shall recognize the Federal agency designated as of
- 22 November 1, 2013, as the ‘Sector Specific Agency’ for
- 23 each critical infrastructure sector designated under sub-
- 24 section (b). If the designated Sector Specific Agency for
- 25 a particular critical infrastructure sector is the Depart-

1 ment, for the purposes of this section, the Secretary shall
2 carry out this section. The Secretary, in coordination with
3 the heads of each such Sector Specific Agency shall—

4 “(1) support the security and resilience activi-
5 ties of the relevant critical infrastructure sector in
6 accordance with this subtitle; and

7 “(2) provide institutional knowledge and spe-
8 cialized expertise to the relevant critical infrastruc-
9 ture sector.

10 “(d) SECTOR COORDINATING COUNCILS.—

11 “(1) RECOGNITION.—The Secretary, in collabo-
12 ration with each critical infrastructure sector and
13 the relevant Sector Specific Agency, shall recognize
14 and partner with the Sector Coordinating Council
15 for each critical infrastructure sector designated
16 under subsection (b) to coordinate with each such
17 sector on security and resilience activities and emer-
18 gency response and recovery efforts.

19 “(2) MEMBERSHIP.—

20 “(A) IN GENERAL.—The Sector Coordi-
21 nating Council for a critical infrastructure sec-
22 tor designated under subsection (b) shall—

23 “(i) be comprised exclusively of rel-
24 evant critical infrastructure owners, critical
25 infrastructure operators, private entities,

1 and representative trade associations for
2 the sector;

3 “(ii) reflect the unique composition of
4 each sector; and

5 “(iii) include relevant small, medium,
6 and large critical infrastructure owners,
7 critical infrastructure operators, private
8 entities, and representative trade associa-
9 tions for the sector.

10 “(B) PROHIBITION.—No government enti-
11 ty with regulating authority shall be a member
12 of the Sector Coordinating Council.

13 “(C) LIMITATION.—The Secretary shall
14 have no role in the determination of the mem-
15 bership of a Sector Coordinating Council.

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

19 “(A) serve as a self-governing, self-orga-
20 nized primary policy, planning, and strategic
21 communications entity for coordinating with the
22 Department, the relevant Sector-Specific Agen-
23 cy designated under subsection (c), and the rel-
24 evant Information Sharing and Analysis Cen-
25 ters under subsection (e) on security and resil-

1 ience activities and emergency response and re-
2 covery efforts;

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

7 “(C) coordinate with the Department, the
8 relevant Information Sharing and Analysis Cen-
9 ters under subsection (e), and other Sector Co-
10 ordinating Councils to update, maintain, and
11 exercise the National Cybersecurity Incident
12 Response Plan in accordance with section
13 229(b); and

14 “(D) provide any recommendations to the
15 Department on infrastructure protection tech-
16 nology gaps to help inform research and devel-
17 opment efforts at the Department.

18 “(e) SECTOR INFORMATION SHARING AND ANALYSIS
19 CENTERS.—

20 “(1) RECOGNITION.—The Secretary, in collabo-
21 ration with the relevant Sector Coordinating Council
22 and the critical infrastructure sector represented by
23 such Council, and in coordination with the relevant
24 Sector Specific Agency, shall recognize at least one
25 Information Sharing and Analysis Center for each

1 critical infrastructure sector designated under sub-
2 section (b) for purposes of paragraph (3). No other
3 Information Sharing and Analysis Organizations, in-
4 cluding Information Sharing and Analysis Centers,
5 may be precluded from having an information shar-
6 ing relationship within the National Cybersecurity
7 and Communications Integration Center established
8 pursuant to section 228. Nothing in this subsection
9 or any other provision of this subtitle may be con-
10 strued to limit, restrict, or condition any private en-
11 tity or activity utilized by, among, or between pri-
12 vate entities.

13 “(2) ROLES AND RESPONSIBILITIES.—In addi-
14 tion to such other activities as may be authorized by
15 law, at least one Information Sharing and Analysis
16 Center for a critical infrastructure sector shall—

17 “(A) serve as an information sharing re-
18 source for such sector and promote ongoing
19 multi-directional sharing of real-time, relevant,
20 and actionable cyber threat information and
21 analysis by and among such sector, the Depart-
22 ment, the relevant Sector Specific Agency, and
23 other critical infrastructure sector Information
24 Sharing and Analysis Centers;

1 “(B) establish governance and operating
2 procedures to carry out the activities conducted
3 under this subsection;

4 “(C) serve as an emergency response and
5 recovery operations coordination point for such
6 sector, and upon request, facilitate cyber inci-
7 dent response capabilities in coordination with
8 the Department, the relevant Sector Specific
9 Agency and the relevant Sector Coordinating
10 Council;

11 “(D) facilitate cross-sector coordination
12 and sharing of cyber threat information to pre-
13 vent related or consequential impacts to other
14 critical infrastructure sectors;

15 “(E) coordinate with the Department, the
16 relevant Sector Coordinating Council, the rel-
17 evant Sector Specific Agency, and other critical
18 infrastructure sector Information Sharing and
19 Analysis Centers on the development, integra-
20 tion, and implementation of procedures to sup-
21 port technology neutral, real-time information
22 sharing capabilities and mechanisms within the
23 National Cybersecurity and Communications
24 Integration Center established pursuant to sec-
25 tion 228, including—

1 “(i) the establishment of a mechanism
2 to voluntarily report identified
3 vulnerabilities and opportunities for im-
4 provement;

5 “(ii) the establishment of metrics to
6 assess the effectiveness and timeliness of
7 the Department’s and Information Sharing
8 and Analysis Centers’ information sharing
9 capabilities; and

10 “(iii) the establishment of a mecha-
11 nism for anonymous suggestions and com-
12 ments;

13 “(F) implement an integration and anal-
14 ysis function to inform sector planning, risk
15 mitigation, and operational activities regarding
16 the protection of each critical infrastructure
17 sector from cyber incidents;

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

22 “(H) coordinate with the Department, the
23 relevant Sector Specific Agency, and the rel-
24 evant Sector Coordinating Council to update,
25 maintain, and exercise the National

1 Cybersecurity Incident Response Plan in ac-
2 cordance with section 229(b); and

3 “(I) safeguard cyber threat information
4 from unauthorized disclosure.

5 “(3) FUNDING.—Of the amounts authorized to
6 be appropriated for each of fiscal years 2014, 2015,
7 and 2016 for the Cybersecurity and Communications
8 Office of the Department, the Secretary is author-
9 ized to use not less than \$25,000,000 for any such
10 year for operations support at the National
11 Cybersecurity and Communications Integration Cen-
12 ter established under section 228(a) of all recognized
13 Information Sharing and Analysis Centers under
14 paragraph (1) of this subsection.

15 “(f) CLEARANCES.—The Secretary—

16 “(1) shall expedite the process of security clear-
17 ances under Executive Order 13549 or successor or-
18 ders for appropriate representatives of Sector Co-
19 ordinating Councils and the critical infrastructure
20 sector Information Sharing and Analysis Centers;
21 and

22 “(2) may so expedite such processing to—

23 “(A) appropriate personnel of critical in-
24 frastructure owners and critical infrastructure
25 operators; and

1 “(B) any other person as determined by
2 the Secretary.

3 “(g) PUBLIC-PRIVATE COLLABORATION.—The Sec-
4 retary, in collaboration with the critical infrastructure sec-
5 tors designated under subsection (b), such sectors’ Sector
6 Specific Agencies recognized under subsection (c), and the
7 Sector Coordinating Councils recognized under subsection
8 (d), shall—

9 “(1) conduct an analysis and review of the ex-
10 isting public-private partnership model and evaluate
11 how the model between the Department and critical
12 infrastructure owners and critical infrastructure op-
13 erators can be improved to ensure the Department,
14 critical infrastructure owners, and critical infrastruc-
15 ture operators are equal partners and regularly col-
16 laborate on all programs and activities of the De-
17 partment to protect critical infrastructure;

18 “(2) develop and implement procedures to en-
19 sure continuous, collaborative, and effective inter-
20 actions between the Department, critical infrastruc-
21 ture owners, and critical infrastructure operators;
22 and

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

1 “(h) PROTECTION OF FEDERAL CIVILIAN INFORMA-
2 TION SYSTEMS.—

3 “(1) IN GENERAL.—The Secretary shall admin-
4 ister the operational information security activities
5 and functions to protect and ensure the resiliency of
6 all Federal civilian information systems.

7 “(2) ROLES AND RESPONSIBILITIES.—The Sec-
8 retary, in coordination with the heads of other Fed-
9 eral civilian agencies, shall—

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

15 “(B) administer Federal Government-wide
16 efforts to develop and provide adequate, risk-
17 based, cost-effective, and technology neutral in-
18 formation security capabilities;

19 “(C) establish and sustain continuous
20 diagnostics systems for Federal civilian infor-
21 mation systems to aggregate data and identify
22 and prioritize the mitigation of cyber
23 vulnerabilities in such systems for cybersecurity
24 purposes;

1 “(D) develop, acquire, and operate an inte-
2 grated and consolidated system of intrusion de-
3 tection, analytics, intrusion prevention, and
4 other information sharing and protective capa-
5 bilities to defend Federal civilian information
6 systems from cyber threats;

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

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

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

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

1 “(I) develop reporting requirements, con-
2 sistent with relevant law, to ensure the National
3 Cybersecurity and Communications Integration
4 Center established pursuant to section 228 re-
5 ceives all actionable cyber threat information
6 identified on Federal civilian information sys-
7 tems;

8 “(J) develop technology neutral perform-
9 ance requirements and metrics for the security
10 of Federal civilian information systems;

11 “(K) implement training requirements that
12 include industry recognized certifications to en-
13 sure that Federal civilian agencies are able to
14 fully and timely comply with policies and proce-
15 dures issued by the Secretary under this sub-
16 section; and

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

22 “(3) USE OF CERTAIN COMMUNICATIONS.—

23 “(A) IN GENERAL.—The Secretary may
24 enter into contracts or other agreements, or
25 otherwise request and obtain, in accordance

1 with applicable law, the assistance of private
2 entities that provide electronic communication
3 services, remote computing services, or
4 cybersecurity services to acquire, intercept, re-
5 tain, use, and disclose communications and
6 other system traffic, deploy countermeasures, or
7 otherwise operate protective capabilities in ac-
8 cordance with subparagraphs (C), (D), (E), and
9 (F) of paragraph (2). No cause of action shall
10 exist against private entities for assistance pro-
11 vided to the Secretary in accordance with this
12 subsection.

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

15 “(i) require or compel any private en-
16 tity to enter in a contract or agreement de-
17 scribed in such subparagraph; or

18 “(ii) authorize the Secretary to take
19 any action with respect to any communica-
20 tions or system traffic transiting or resid-
21 ing on any information system or network
22 of information systems other than a Fed-
23 eral civilian information system.

24 “(i) RECOMMENDATIONS REGARDING NEW AGREE-
25 MENTS.—Not later than 180 days after the date of the

1 enactment of this section, the Secretary shall submit to
2 the appropriate congressional committees recommenda-
3 tions on how to expedite the implementation of informa-
4 tion sharing agreements for cybersecurity purposes be-
5 tween the Secretary and critical information owners and
6 critical infrastructure operators and other private entities.
7 Such recommendations shall address the development and
8 utilization of a scalable form that retains all privacy and
9 other protections in such agreements in existence as of
10 such date, including Cooperative and Research Develop-
11 ment Agreements. Such recommendations should also in-
12 clude any additional authorities or resources that may be
13 needed to carry out the implementation of any such new
14 agreements.

15 “(j) RULE OF CONSTRUCTION.—No provision of this
16 title may be construed as modifying, limiting, or otherwise
17 affecting the authority of any other Federal agency under
18 any other provision of law.”.

19 (b) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of such Act is amended by adding after
21 the item relating to section 226 (as added by section 102)
22 the following new item:

“Sec. 227. Protection of critical infrastructure and information sharing.”.

1 **SEC. 104. NATIONAL CYBERSECURITY AND COMMUNICA-**
2 **TIONS INTEGRATION CENTER.**

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

7 **“SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICA-**
8 **TIONS INTEGRATION CENTER.**

9 “(a) ESTABLISHMENT.—There is established in the
10 Department the National Cybersecurity and Communica-
11 tions Integration Center (referred to in this section as the
12 ‘Center’), which shall be a Federal civilian information
13 sharing interface that provides shared situational aware-
14 ness to enable real-time, integrated, and operational ac-
15 tions across the Federal Government, and share cyber
16 threat information by and among Federal, State, and local
17 government entities, Information Sharing and Analysis
18 Centers, private entities, and critical infrastructure owners
19 and critical infrastructure operators that have an informa-
20 tion sharing relationship with the Center.

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

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

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

4 “(3) The United States Computer Emergency
5 Readiness Team to coordinate cyber threat informa-
6 tion sharing, proactively manage cyber risks to the
7 United States, collaboratively respond to cyber inci-
8 dents, provide technical assistance to information
9 system owners and operators, and disseminate time-
10 ly notifications regarding current and potential cyber
11 threats and vulnerabilities.

12 “(4) The Industrial Control System Cyber
13 Emergency Response Team to coordinate with in-
14 dustrial control systems owners and operators and
15 share industrial control systems-related security inci-
16 dents and mitigation measures.

17 “(5) The National Coordinating Center for
18 Telecommunications to coordinate the protection, re-
19 sponse, and recovery of national security emergency
20 communications.

21 “(6) Such other Federal, State, and local gov-
22 ernment entities, private entities, organizations, or
23 individuals as the Secretary may consider appro-
24 priate that agree to be included.

1 “(c) CYBER INCIDENT.—In the event of a cyber inci-
2 dent, the Secretary may grant the entities referred to in
3 subsection (a) immediate temporary access to the Center
4 as a situation may warrant.

5 “(d) ROLES AND RESPONSIBILITIES.—The Center
6 shall—

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

14 “(2) coordinate with other Federal agencies to
15 streamline and reduce redundant reporting of cyber
16 threat information;

17 “(3) provide, upon request, timely technical as-
18 sistance and crisis management support to Federal,
19 State, and local government entities and private en-
20 tities that own or operate information systems or
21 networks of information systems to protect from,
22 prevent, mitigate, respond to, and recover from
23 cyber incidents;

24 “(4) facilitate cross-sector coordination and
25 sharing of cyber threat information to prevent re-

1 lated or consequential impacts to other critical infra-
2 structure sectors;

3 “(5) collaborate with the Sector Coordinating
4 Councils, Information Sharing and Analysis Centers,
5 Sector Specific Agencies, and the relevant critical in-
6 frastructure sectors on the development and imple-
7 mentation of procedures to support technology neu-
8 tral real-time information sharing capabilities and
9 mechanisms;

10 “(6) collaborate with the Sector Coordinating
11 Councils, Information Sharing and Analysis Centers,
12 Sector Specific Agencies, and the relevant critical in-
13 frastructure sectors to identify requirements for data
14 and information formats and accessibility, system
15 interoperability, and redundant systems and alter-
16 native capabilities in the event of a disruption in the
17 primary information sharing capabilities and mecha-
18 nisms at the Center;

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

22 “(8) safeguard sensitive cyber threat informa-
23 tion from unauthorized disclosure;

24 “(9) require other Federal civilian agencies to—

1 “(A) send reports and information to the
2 Center about cyber incidents, threats, and
3 vulnerabilities affecting Federal civilian infor-
4 mation systems and critical infrastructure sys-
5 tems and, in the event a private vendor product
6 or service of such an agency is so implicated,
7 the Center shall first notify such private vendor
8 of the vulnerability before further disclosing
9 such information;

10 “(B) provide to the Center cyber incident
11 detection, analysis, mitigation, and response in-
12 formation; and

13 “(C) immediately send and disclose to the
14 Center cyber threat information received by
15 such agencies;

16 “(10) perform such other duties as the Sec-
17 retary may require to facilitate a national effort to
18 strengthen and maintain secure, functioning, and re-
19 silient critical infrastructure from cyber threats; and

20 “(11) implement policies and procedures to—

21 “(A) provide technical assistance to Fed-
22 eral civilian agencies to prevent and respond to
23 data breaches involving unauthorized acquisi-
24 tion or access of personally identifiable informa-

1 tion that occur on Federal civilian information
2 systems;

3 “(B) require Federal civilian agencies to
4 notify the Center about data breaches involving
5 unauthorized acquisition or access of personally
6 identifiable information that occur on Federal
7 civilian information systems not later than two
8 business days after the discovery of such a
9 breach; and

10 “(C) require Federal civilian agencies to
11 notify all potential victims of a data breach in-
12 volving unauthorized acquisition or access of
13 personally identifiable information that occur on
14 Federal civilian information systems without
15 unreasonable delay consistent with the needs of
16 law enforcement.

17 “(e) INTEGRATION AND ANALYSIS.—The Center
18 shall maintain an integration and analysis function, which
19 shall —

20 “(1) integrate and analyze all cyber threat in-
21 formation received from other Federal agencies,
22 State and local governments, Information Sharing
23 and Analysis Centers, private entities, critical infra-
24 structure owners, and critical infrastructure opera-

1 tors, and share relevant information in near real-
2 time;

3 “(2) on an ongoing basis, assess and evaluate
4 consequence, vulnerability, and threat information to
5 share with the entities referred to in subsection (a)
6 actionable assessments of critical infrastructure sec-
7 tor risks from cyber incidents and to assist critical
8 infrastructure owners and critical infrastructure op-
9 erators by making recommendations to facilitate
10 continuous improvements to the security and resil-
11 iency of the critical infrastructure of the United
12 States;

13 “(3) facilitate cross-sector integration, identi-
14 fication, and analysis of key interdependencies to
15 prevent related or consequential impacts to other
16 critical infrastructure sectors; and

17 “(4) collaborate with the Information Sharing
18 and Analysis Centers to tailor the analysis of infor-
19 mation to the specific characteristics and risk to a
20 relevant critical infrastructure sector.

21 “(f) REPORT OF CYBER ATTACKS AGAINST FEDERAL
22 GOVERNMENT NETWORKS.—The Secretary shall submit
23 to the Committee on Homeland Security of the House of
24 Representatives, the Committee on Homeland Security
25 and Governmental Affairs of the Senate, and the Comp-

1 troller General of the United States an annual report that
2 summarizes major cyber incidents involving Federal civil-
3 ian agency information systems and provides aggregate
4 statistics on the number of breaches, the extent of any
5 personally identifiable information that was involved, the
6 volume of data exfiltrated, the consequential impact, and
7 the estimated cost of remedying such breaches.

8 “(g) REPORT ON THE OPERATIONS OF THE CEN-
9 TER.—The Secretary, in consultation with the Sector Co-
10 ordinating Councils and appropriate Federal Government
11 entities, shall submit to the Committee on Homeland Se-
12 curity of the House of Representatives, the Committee on
13 Homeland Security and Governmental Affairs of the Sen-
14 ate, and the Comptroller General of the United States an
15 annual report on—

16 “(1) the capability and capacity of the Center
17 to carry out its cybersecurity mission in accordance
18 with this section, and sections 226, 227, 229, 230,
19 230A, and 230B;

20 “(2) the extent to which the Department is en-
21 gaged in information sharing with each critical in-
22 frastructure sector designated under section 227(b),
23 including—

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

1 “(B) the extent to which critical infra-
2 structure owners and critical infrastructure op-
3 erators of each critical infrastructure sector
4 participate in information sharing at the Cen-
5 ter;

6 “(3) the volume and range of activities with re-
7 spect to which the Secretary collaborated with the
8 Sector Coordinating Councils and the Sector-Specific
9 Agencies to promote greater engagement with the
10 Center; and

11 “(4) the volume and range of voluntary tech-
12 nical assistance sought and provided by the Depart-
13 ment to each critical infrastructure owner and crit-
14 ical infrastructure operator.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of such Act is amended by adding after
17 the item relating to section 227 (as added by section 103)
18 the following new item:

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

19 (c) GAO REPORT.—Not later than one year after the
20 date of the enactment of this Act, the Comptroller General
21 of the United States shall submit to the Committee on
22 Homeland Security of the House of Representatives and
23 the Committee on Homeland Security and Governmental
24 Affairs of the Senate a report on the effectiveness of the
25 National Cybersecurity and Communications Integration

1 Center established under section 228 of the Homeland Se-
2 curity Act of 2002, as added by subsection (a) of this sec-
3 tion, in carrying out its cybersecurity mission (as such
4 term is defined in section 2 of the Homeland Security Act
5 of 2002, as amended by section 101) in accordance with
6 this Act and such section 228 and sections 226, 227, 229,
7 230, 230A, and 230B of the Homeland Security Act of
8 2002, as added by this Act.

9 **SEC. 105. CYBER INCIDENT RESPONSE AND TECHNICAL AS-**
10 **SISTANCE.**

11 (a) IN GENERAL.—Subtitle C of title II of the Home-
12 land Security Act of 2002, as amended by sections 102,
13 103, and 104, is further amended by adding at the end
14 the following new section:

15 **“SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL**
16 **ASSISTANCE.**

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

19 “(1) upon request, provide timely technical as-
20 sistance and crisis management support to Federal,
21 State, and local government entities, private entities,
22 and critical infrastructure owners and critical infra-
23 structure operators involving cyber incidents affect-
24 ing critical infrastructure; and

1 “(2) upon request, provide actionable rec-
2 ommendations on security and resilience measures
3 and countermeasures to Federal, State, and local
4 government entities, private entities, and critical in-
5 frastructure owners and critical infrastructure oper-
6 ators prior to, during, and after cyber incidents.

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

10 “(c) CYBER INCIDENT RESPONSE PLAN.—The Sec-
11 retary, in coordination with the Sector Coordinating Coun-
12 cils, Information Sharing and Analysis Centers, and Fed-
13 eral, State, and local governments, shall develop, regularly
14 update, maintain, and exercise a National Cybersecurity
15 Incident Response Plan which shall—

16 “(1) include effective emergency response plans
17 associated with cyber threats to critical infrastruc-
18 ture, information systems, or networks of informa-
19 tion systems; and

20 “(2) ensure that such National Cybersecurity
21 Incident Response Plan can adapt to and reflect a
22 changing cyber threat environment, and incorporate
23 best practices and lessons learned from regular exer-
24 cises, training, and after-action reports.”.

1 (b) CLERICAL AMENDMENT.—The table of contents
2 in section 1(b) of such Act is amended by adding after
3 the item relating to section 228 (as added by section 104)
4 the following new item:

“229. Cyber incident response and technical assistance.”.

5 **SEC. 106. STREAMLINING OF DEPARTMENT**
6 **CYBERSECURITY ORGANIZATION.**

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

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

20 (1) IN GENERAL.—Subsection (a) of section
21 103 of the Homeland Security Act of 2002 (6
22 U.S.C. 113) is amended by adding at the end the
23 following new subparagraphs:

24 “(K) Under Secretary for Cybersecurity
25 and Infrastructure Protection.

1 “(L) Deputy Under Secretary for
2 Cybersecurity.

3 “(M) Deputy Under Secretary for Infra-
4 structure Protection.”.

5 (2) CONTINUATION IN OFFICE.—The individ-
6 uals who hold the positions referred to in subpara-
7 graphs (K), (L), and (M) of subsection (a) of section
8 103 of the Homeland Security Act of 2002 (as
9 added by paragraph (1) of this subsection) as of the
10 date of the enactment of this Act may continue to
11 hold such positions.

12 (c) REPORT ON IMPROVING THE CAPABILITY AND
13 EFFECTIVENESS OF THE CYBERSECURITY AND COMMU-
14 NICATIONS OFFICE.—To improve the operational capa-
15 bility and effectiveness in carrying out the cybersecurity
16 mission (as such term is defined in section 2 of the Home-
17 land Security Act of 2002, as amended by section 101)
18 of the Department of Homeland Security, the Secretary
19 of Homeland Security shall submit to the Committee on
20 Homeland Security of the House of Representatives and
21 the Committee on Homeland Security and Governmental
22 Affairs of the Senate a report on—

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

1 (2) recommendations for restructuring the
2 SAFETY Act Office within the Department to pro-
3 tect and maintain operations in accordance with the
4 Office's mission to provide incentives for the devel-
5 opment and deployment of anti-terrorism tech-
6 nologies while elevating the profile and mission of
7 the Office, including the feasibility of utilizing third-
8 party registrars for improving the throughput and
9 effectiveness of the certification process.

10 (d) REPORT ON CYBERSECURITY ACQUISITION CAPA-
11 BILITIES.—The Secretary of Homeland Security shall as-
12 sess the effectiveness of the Department of Homeland Se-
13 curity's acquisition processes and the use of existing au-
14 thorities for acquiring cybersecurity technologies to ensure
15 that such processes and authorities are capable of meeting
16 the needs and demands of the Department's cybersecurity
17 mission (as such term is defined in section 2 of the Home-
18 land Security Act of 2002, as amended by section 101).
19 Not later than 180 days after the date of the enactment
20 of this Act, the Secretary shall submit to the Committee
21 on Homeland Security of the House of Representatives
22 and the Committee on Homeland Security and Govern-
23 mental Affairs of the Senate a report on the effectiveness
24 of the Department's acquisition processes for
25 cybersecurity technologies.

1 **TITLE II—PUBLIC-PRIVATE COL-**
2 **LABORATION** **ON**
3 **CYBERSECURITY**

4 **SEC. 201. PUBLIC-PRIVATE COLLABORATION ON**
5 **CYBERSECURITY.**

6 (a) NATIONAL INSTITUTE OF STANDARDS AND
7 TECHNOLOGY.—

8 (1) IN GENERAL.—The Director of the National
9 Institute of Standards and Technology, in coordina-
10 tion with the Secretary of Homeland Security, shall,
11 on an ongoing basis, facilitate and support the devel-
12 opment of a voluntary, industry-led set of standards,
13 guidelines, best practices, methodologies, procedures,
14 and processes to reduce cyber risks to critical infra-
15 structure. The Director, in coordination with the
16 Secretary—

17 (A) shall—

18 (i) coordinate closely and continuously
19 with relevant private entities, critical infra-
20 structure owners and critical infrastructure
21 operators, Sector Coordinating Councils,
22 Information Sharing and Analysis Centers,
23 and other relevant industry organizations,
24 and incorporate industry expertise to the
25 fullest extent possible;

- 1 (ii) consult with the Sector Specific
2 Agencies, Federal, State and local govern-
3 ments, the governments of other countries,
4 and international organizations;
- 5 (iii) utilize a prioritized, flexible, re-
6 peatable, performance-based, and cost-ef-
7 fective approach, including information se-
8 curity measures and controls, that may be
9 voluntarily adopted by critical infrastruc-
10 ture owners and critical infrastructure op-
11 erators to help them identify, assess, and
12 manage cyber risks;
- 13 (iv) include methodologies to—
- 14 (I) identify and mitigate impacts
15 of the cybersecurity measures or con-
16 trols on business confidentiality; and
- 17 (II) protect individual privacy
18 and civil liberties;
- 19 (v) incorporate voluntary consensus
20 standards and industry best practices, and
21 align with voluntary international stand-
22 ards to the fullest extent possible;
- 23 (vi) prevent duplication of existing
24 regulatory processes and prevent conflict

1 with or superseding of existing regulatory
2 requirements and processes; and

3 (vii) include such other similar and
4 consistent elements as determined nec-
5 essary; and

6 (B) shall not prescribe or otherwise re-
7 quire—

8 (i) the use of specific solutions;

9 (ii) the use of specific information
10 technology products or services; or

11 (iii) that information technology prod-
12 ucts or services be designed, developed, or
13 manufactured in a particular manner.

14 (2) LIMITATION.—Information shared with or
15 provided to the Director of the National Institute of
16 Standards and Technology or the Secretary of
17 Homeland Security for the purpose of the activities
18 under paragraph (1) may not be used by any Fed-
19 eral, State, or local government department or agen-
20 cy to regulate the activity of any private entity.

21 (b) AMENDMENT.—

22 (1) IN GENERAL.—Subtitle C of title II of the
23 Homeland Security Act of 2002, as amended by sec-
24 tions 102, 103, 104, and 105, is further amended by
25 adding at the end the following new section:

1 **“SEC. 230. PUBLIC-PRIVATE COLLABORATION ON**
2 **CYBERSECURITY.**

3 “(a) MEETINGS.—The Secretary shall meet with the
4 Sector Coordinating Council for each critical infrastruc-
5 ture sector designated under section 227(b) on a biannual
6 basis to discuss the cybersecurity threat to critical infra-
7 structure, voluntary activities to address cybersecurity,
8 and ideas to improve the public-private partnership to en-
9 hance cybersecurity, in which the Secretary shall—

10 “(1) provide each Sector Coordinating Council
11 an assessment of the cybersecurity threat to each
12 critical infrastructure sector designated under sec-
13 tion 227(b), including information relating to—

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

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

23 “(C) the threat to national security caused
24 by an act of terrorism or other disruption, de-
25 struction, or unauthorized use of critical infra-
26 structure; and

1 “(D) the harm to the economy that would
2 result from an act of terrorism or other disrup-
3 tion, destruction, or unauthorized use of critical
4 infrastructure; and

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

8 “(b) REPORT.—

9 “(1) IN GENERAL.—Starting 30 days after the
10 end of the fiscal year in which the National
11 Cybersecurity and Critical Infrastructure Protection
12 Act of 2013 is enacted and annually thereafter, the
13 Secretary shall submit to the appropriate congress-
14 sional committees a report on the state of
15 cybersecurity for each critical infrastructure sector
16 designated under section 227(b) based on discus-
17 sions between the Department and the Sector Co-
18 ordinating Council in accordance with subsection (a)
19 of this section. The Secretary shall maintain a public
20 copy of each report, and each report may include a
21 non-public annex for proprietary, business-sensitive
22 information, or other sensitive information. Each re-
23 port shall include, at a minimum information relat-
24 ing to—

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

4 “(B) the extent and nature of any
5 cybersecurity incidents during the previous
6 year, including the extent to which cyber inci-
7 dents jeopardized or imminently jeopardized in-
8 formation systems;

9 “(C) the current status of the voluntary,
10 industry-led set of standards, guidelines, best
11 practices, methodologies, procedures, and proc-
12 esses to reduce cyber risks within each critical
13 infrastructure sector; and

14 “(D) the volume and range of voluntary
15 technical assistance sought and provided by the
16 Department to each critical infrastructure sec-
17 tor.

18 “(2) SECTOR COORDINATING COUNCIL RE-
19 SPONSE.—Before making public and submitting
20 each report required under paragraph (1), the Sec-
21 retary shall provide a draft of each report to the
22 Sector Coordinating Council for the critical infra-
23 structure sector covered by each such report. The
24 Sector Coordinating Council at issue may provide to
25 the Secretary a written response to such report with-

1 in 45 days of receiving the draft. If such Sector Co-
2 ordinating Council provides a written response, the
3 Secretary shall include such written response in the
4 final version of each report required under para-
5 graph (1).

6 “(c) LIMITATION.—Information shared with or pro-
7 vided to a Sector Coordinating Council, a critical infra-
8 structure sector, or the Secretary for the purpose of the
9 activities under subsections (a) and (b) may not be used
10 by any Federal, State, or local government department or
11 agency to regulate the activity of any private entity.”.

12 (2) CLERICAL AMENDMENT.—The table of con-
13 tents in section 1(b) of such Act is amended by add-
14 ing after the item relating to section 229 (as added
15 by section 105) the following new item:

“Sec. 230. Public-private collaboration on cybersecurity.”.

16 **SEC. 202. SAFETY ACT AND QUALIFYING CYBER INCIDENTS.**

17 (a) IN GENERAL.—The Support Anti-Terrorism By
18 Fostering Effective Technologies Act of 2002 (6 U.S.C.
19 441 et seq.) is amended—

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

21 (A) in the heading, by striking “DESIGNA-
22 TION OF QUALIFIED ANTI-TERRORISM TECH-
23 NOLOGIES” and inserting “DESIGNATION OF
24 ANTI-TERRORISM AND CYBERSECURITY TECH-
25 NOLOGIES”;

1 (B) in the matter preceding paragraph (1),
2 by inserting “and cybersecurity” after “anti-
3 terrorism”;

4 (C) in paragraphs (3), (4), and (5), by in-
5 serting “or cybersecurity” after “anti-ter-
6 rorism” each place it appears; and

7 (D) in paragraph (7)—

8 (i) by inserting “or cybersecurity tech-
9 nology” after “Anti-terrorism technology”;
10 and

11 (ii) by inserting “or qualifying cyber
12 incidents” after “acts of terrorism”;

13 (2) in section 863 (6 U.S.C. 442)—

14 (A) by inserting “or cybersecurity” after
15 “anti-terrorism” each place it appears;

16 (B) by inserting “or qualifying cyber inci-
17 dent” after “act of terrorism” each place it ap-
18 pears; and

19 (C) by inserting “or qualifying cyber inci-
20 dents” after “acts of terrorism” each place it
21 appears;

22 (3) in section 864 (6 U.S.C. 443)—

23 (A) by inserting “or cybersecurity” after
24 “anti-terrorism” each place it appears; and

1 (B) by inserting “or qualifying cyber inci-
2 dent” after “act of terrorism” each place it ap-
3 pears; and

4 (4) in section 865 (6 U.S.C. 444)—

5 (A) in paragraph (1)—

6 (i) in the heading, by inserting “OR
7 CYBERSECURITY” after “ANTI-TER-
8 RORISM”;

9 (ii) by inserting “or cybersecurity”
10 after “anti-terrorism”; and

11 (iii) by inserting “or qualifying cyber
12 incident” after “acts of terrorism”; and

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

15 “(7) QUALIFYING CYBER INCIDENT.—

16 “(A) IN GENERAL.—The term ‘qualifying
17 cyber incident’ means any act that the Sec-
18 retary determines meets the requirements under
19 subparagraph (B), as such requirements are
20 further defined and specified by the Secretary.

21 “(B) REQUIREMENTS.—A qualifying cyber
22 incident meets the requirements of this sub-
23 paragraph if—

24 “(i) the incident is unlawful or other-
25 wise exceeds authorized access authority;

1 “(ii) the incident disrupts or immi-
2 nently jeopardizes the integrity, operation,
3 confidentiality, or availability of program-
4 mable electronic devices, communication
5 networks, including hardware, software
6 and data that are essential to their reliable
7 operation, electronic storage devices, or
8 any other information system, or the infor-
9 mation that system controls, processes,
10 stores, or transmits;

11 “(iii) the perpetrator of the incident
12 gains access to an information system or a
13 network of information systems resulting
14 in—

15 “(I) misappropriation or theft of
16 data, assets, information, or intellec-
17 tual property;

18 “(II) corruption of data, assets,
19 information, or intellectual property;

20 “(III) operational disruption; or

21 “(IV) an adverse effect on such
22 system or network, or the data, as-
23 sets, information, or intellectual prop-
24 erty contained therein; and

1 “(iv) the incident causes harm inside
2 or outside the United States that results in
3 material levels of damage, disruption, or
4 casualties severely affecting the United
5 States population, infrastructure, economy,
6 or national morale, or Federal, State, local,
7 or tribal government functions.

8 “(C) RULE OF CONSTRUCTION.—For pur-
9 poses of clause (iv) of subparagraph (B), the
10 term ‘severely’ includes any qualifying cyber in-
11 cident, whether at a local, regional, state, na-
12 tional, international, or tribal level, that af-
13 fects—

14 “(i) the United States population, in-
15 frastructure, economy, or national morale,
16 or

17 “(ii) Federal, State, local, or tribal
18 government functions.”.

19 (b) FUNDING.—Of the amounts authorized to be ap-
20 propriated for each of fiscal years 2014, 2015, and 2016
21 for the Department of Homeland Security, the Secretary
22 of Homeland Security is authorized to use not less than
23 \$20,000,000 for any such year for the Department’s
24 SAFETY Act Office.

1 **SEC. 203. PROHIBITION ON NEW REGULATORY AUTHORITY.**

2 This Act and the amendments made by this Act (ex-
3 cept that this section shall not apply in the case of section
4 202 of this Act and the amendments made by such section
5 202) do not—

6 (1) create or authorize the issuance of any new
7 regulations or additional Federal Government regu-
8 latory authority; or

9 (2) permit regulatory actions that would dupli-
10 cate, conflict with, or supercede existing regulatory
11 requirements, mandatory standards, or related proc-
12 esses.

13 **SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION**
14 **OF APPROPRIATIONS.**

15 No additional funds are authorized to be appro-
16 priated to carry out this Act and the amendments made
17 by this Act. This Act and such amendments shall be car-
18 ried out using amounts otherwise available for such pur-
19 poses.

20 **SEC. 205. PROHIBITION ON COLLECTION ACTIVITIES TO**
21 **TRACK INDIVIDUALS' PERSONALLY IDENTIFI-**
22 **ABLE INFORMATION.**

23 Nothing in this Act shall permit the Department of
24 Homeland Security to engage in the monitoring, surveil-
25 lance, exfiltration, or other collection activities for the pur-

1 pose of tracking an individual's personally identifiable in-
2 formation.

3 **TITLE III—HOMELAND SECURITY**
4 **RITY CYBERSECURITY WORK-**
5 **FORCE**

6 **SEC. 301. HOMELAND SECURITY CYBERSECURITY WORK-**
7 **FORCE.**

8 (a) IN GENERAL.—Subtitle C of title II of the Home-
9 land Security Act of 2002, as amended by sections 101,
10 102, 103, 104, 105, and 201, is further amended by add-
11 ing at the end the following new section:

12 **“SEC. 230A. CYBERSECURITY OCCUPATION CATEGORIES,**
13 **WORKFORCE ASSESSMENT, AND STRATEGY.**

14 “(a) SHORT TITLE.—This section may be referred to
15 as the ‘Homeland Security Cybersecurity Boots-on-the-
16 Ground Act’.

17 “(b) CYBERSECURITY OCCUPATION CATEGORIES.—

18 “(1) IN GENERAL.—Not later than 90 days
19 after the date of the enactment of this section, the
20 Secretary shall develop and issue comprehensive oc-
21 cupation categories for individuals performing activi-
22 ties in furtherance of the cybersecurity mission of
23 the Department.

24 “(2) APPLICABILITY.—The Secretary shall en-
25 sure that the comprehensive occupation categories

1 issued under paragraph (1) are used throughout the
2 Department and are made available to other Federal
3 agencies.

4 “(c) CYBERSECURITY WORKFORCE ASSESSMENT.—

5 “(1) IN GENERAL.—Not later than 180 days
6 after the date of the enactment of this section and
7 annually thereafter, the Secretary shall assess the
8 readiness and capacity of the workforce of the De-
9 partment to meet its cybersecurity mission.

10 “(2) CONTENTS.—The assessment required
11 under paragraph (1) shall, at a minimum, include
12 the following:

13 “(A) Information where cybersecurity posi-
14 tions are located within the Department, speci-
15 fied in accordance with the cybersecurity occu-
16 pation categories issued under subsection (b).

17 “(B) Information on which cybersecurity
18 positions are—

19 “(i) performed by—

20 “(I) permanent full time depart-
21 mental employees, together with de-
22 mographic information about such
23 employees’ race, ethnicity, gender, dis-
24 ability status, and veterans status;

1 “(II) individuals employed by
2 independent contractors; and

3 “(III) individuals employed by
4 other Federal agencies, including the
5 National Security Agency; and

6 “(ii) vacant.

7 “(C) The number of individuals hired by
8 the Department pursuant to the authority
9 granted to the Secretary in 2009 to permit the
10 Secretary to fill 1,000 cybersecurity positions
11 across the Department over a three year period,
12 and information on what challenges, if any,
13 were encountered with respect to the implemen-
14 tation of such authority.

15 “(D) Information on vacancies within the
16 Department’s cybersecurity supervisory work-
17 force, from first line supervisory positions
18 through senior departmental cybersecurity posi-
19 tions.

20 “(E) Information on the percentage of in-
21 dividuals within each cybersecurity occupation
22 category who received essential training to per-
23 form their jobs, and in cases in which such
24 training is not received, information on what

1 challenges, if any, were encountered with re-
2 spect to the provision of such training.

3 “(F) Information on recruiting costs in-
4 curred with respect to efforts to fill
5 cybersecurity positions across the Department
6 in a manner that allows for tracking of overall
7 recruiting and identifying areas for better co-
8 ordination and leveraging of resources within
9 the Department.

10 “(d) WORKFORCE STRATEGY.—

11 “(1) IN GENERAL.—Not later than 180 days
12 after the date of the enactment of this section, the
13 Secretary shall develop, maintain, and, as necessary,
14 update, a comprehensive workforce strategy that en-
15 hances the readiness, capacity, training, recruitment,
16 and retention of the cybersecurity workforce of the
17 Department.

18 “(2) CONTENTS.—The comprehensive work-
19 force strategy developed under paragraph (1) shall
20 include—

21 “(A) a multiphased recruitment plan, in-
22 cluding relating to experienced professionals,
23 members of disadvantaged or underserved com-
24 munities, the unemployed, and veterans;

25 “(B) a 5-year implementation plan;

1 “(C) a 10-year projection of the Depart-
2 ment’s cybersecurity workforce needs; and

3 “(D) obstacles impeding the hiring and de-
4 velopment of a cybersecurity workforce at the
5 Department.

6 “(e) INFORMATION SECURITY TRAINING.—Not later
7 than 270 days after the date of the enactment of this sec-
8 tion, the Secretary shall establish and maintain a process
9 to verify on an ongoing basis that individuals employed
10 by independent contractors who serve in cybersecurity po-
11 sitions at the Department receive initial and recurrent in-
12 formation security training comprised of general security
13 awareness training necessary to perform their job func-
14 tions, and role-based security training that is commensu-
15 rate with assigned responsibilities. The Secretary shall
16 maintain documentation to ensure that training provided
17 to an individual under this subsection meets or exceeds
18 requirements for such individual’s job function.

19 “(f) UPDATES.—The Secretary shall submit to the
20 appropriate congressional committees annual updates re-
21 garding the cybersecurity workforce assessment required
22 under subsection (c), information on the progress of car-
23 rying out the comprehensive workforce strategy developed
24 under subsection (d), and information on the status of the

1 implementation of the information security training re-
2 quired under subsection (e).

3 “(g) GAO STUDY.—The Secretary shall provide the
4 Comptroller General of the United States with information
5 on the cybersecurity workforce assessment required under
6 subsection (c) and progress on carrying out the com-
7 prehensive workforce strategy developed under subsection
8 (d). The Comptroller General shall submit to the Sec-
9 retary and the appropriate congressional committees a
10 study on such assessment and strategy.

11 “(h) CYBERSECURITY FELLOWSHIP PROGRAM.—Not
12 later than 120 days after the date of the enactment of
13 this section, the Secretary shall submit to the appropriate
14 congressional committees a report on the feasibility of es-
15 tablishing a Cybersecurity Fellowship Program to offer a
16 tuition payment plan for undergraduate and doctoral can-
17 didates who agree to work for the Department for an
18 agreed-upon period of time.”.

19 (b) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of such Act is amended by adding after
21 the item relating to section 230 (as added by section 201)
22 the following new item:

“Sec. 230A. Cybersecurity occupation categories, workforce assessment, and
strategy.”.

1 **SEC. 302. PERSONNEL AUTHORITIES.**

2 (a) IN GENERAL.—Subtitle C of title II of the Home-
3 land Security Act of 2002, as amended by sections 101,
4 102, 103, 104, 105, 106, 201, and 301 is further amended
5 by adding at the end the following new section:

6 **“SEC. 230B. PERSONNEL AUTHORITIES.**

7 “(a) IN GENERAL.—

8 “(1) PERSONNEL AUTHORITIES.—The Sec-
9 retary may exercise with respect to qualified employ-
10 ees of the Department the same authority that the
11 Secretary of Defense has with respect to civilian in-
12 telligence personnel and the scholarship program
13 under sections 1601, 1602, 1603, and 2200a of title
14 10, United States Code, to establish as positions in
15 the excepted service, appoint individuals to such po-
16 sitions, fix pay, and pay a retention bonus to any
17 employee appointed under this section if the Sec-
18 retary determines that such is needed to retain es-
19 sential personnel. Before announcing the payment of
20 a bonus under this paragraph, the Secretary shall
21 submit to the Committee on Homeland Security of
22 the House of Representatives and the Committee on
23 Homeland Security and Governmental Affairs of the
24 Senate a written explanation of such determination.
25 Such authority shall be exercised—

1 “(A) to the same extent and subject to the
2 same conditions and limitations that the Sec-
3 retary of Defense may exercise such authority
4 with respect to civilian intelligence personnel of
5 the Department of Defense; and

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

9 “(2) CIVIL SERVICE PROTECTIONS.—Sections
10 1221 and 2302, and chapter 75 of title 5, United
11 States Code, shall apply to the positions established
12 pursuant to the authorities provided under para-
13 graph (1).

14 “(3) PLAN FOR EXECUTION OF AUTHORI-
15 TIES.—Not later than 120 days after the date of the
16 enactment of this section, the Secretary shall submit
17 to the Committee on Homeland Security of the
18 House of Representatives and the Committee on
19 Homeland Security and Governmental Affairs of the
20 Senate a report that contains a plan for the use of
21 the authorities provided under this subsection.

22 “(b) ANNUAL REPORT.—Not later than one year
23 after the date of the enactment of this section and annu-
24 ally thereafter for four years, the Secretary shall submit
25 to the Committee on Homeland Security of the House of

1 Representatives and the Committee on Homeland Security
2 and Governmental Affairs of the Senate a detailed report
3 (including appropriate metrics on actions occurring during
4 the reporting period) that discusses the processes used by
5 the Secretary in implementing this section and accepting
6 applications, assessing candidates, ensuring adherence to
7 veterans' preference, and selecting applicants for vacancies
8 to be filled by a qualified employee.

9 “(c) DEFINITION OF QUALIFIED EMPLOYEE.—In
10 this section, the term ‘qualified employee’ means an em-
11 ployee who performs functions relating to the security of
12 Federal civilian information systems, critical infrastruc-
13 ture information systems, or networks of either of such
14 systems.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of such Act is amended by adding after
17 the item relating to section 230A (as added by section
18 301) the following new item:

“230B. Personnel authorities.”.

