

113TH CONGRESS
2^D SESSION

H. R. 3696

AN ACT

To amend the Homeland Security Act of 2002 to make certain improvements 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,*

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.
- Sec. 206. Cybersecurity scholars.
- Sec. 207. National Research Council study on the resilience and reliability of the Nation’s power grid.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

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

6 **TITLE I—SECURING THE NATION**
7 **AGAINST CYBER ATTACK**

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

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

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

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

6 “(21) The term ‘critical infrastructure operator’
7 means a critical infrastructure owner or other per-
8 son that manages, runs, or operates, in whole or in
9 part, the day-to-day operations of critical infrastruc-
10 ture.

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

14 “(A) jeopardize or imminently jeopardize,
15 without lawful authority, the security, integrity,
16 confidentiality, or availability of an information
17 system or network of information systems or
18 any information stored on, processed on, or
19 transiting such a system or network;

20 “(B) constitute a violation or imminent
21 threat of violation of law, security policies, secu-
22 rity procedures, or acceptable use policies re-
23 lated to such a system or network, or an act of
24 terrorism against such a system or network; or

1 “(C) result in the denial of access to or
2 degradation, disruption, or destruction of such
3 a system or network, or the defeat of an oper-
4 ations control or technical control essential to
5 the security or operation of such a system or
6 network.

7 “(23) The term ‘cybersecurity mission’ means
8 activities that encompass the full range of threat re-
9 duction, vulnerability reduction, deterrence, incident
10 response, resiliency, and recovery activities to foster
11 the security and stability of cyberspace.

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

19 “(A) a vulnerability of such a system or
20 network;

21 “(B) a threat to the security, integrity,
22 confidentiality, or availability of such a system
23 or network, or any information stored on, proc-
24 essed on, or transiting such a system or net-
25 work;

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

3 “(D) efforts to gain unauthorized access to
4 such a system or network, including to gain
5 such unauthorized access for the purpose of
6 exfiltrating information stored on, processed on,
7 or transiting such a system or network.

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

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

18 “(A) a vulnerability of an information sys-
19 tem or network of information systems of a
20 government or private entity;

21 “(B) a threat to the security, integrity,
22 confidentiality, or availability of such a system
23 or network of a government or private entity, or
24 any information stored on, processed on, or
25 transiting such a system or network;

1 “(C) efforts to deny access to or degrade,
2 disrupt, or destroy such a system or network of
3 a government or private entity;

4 “(D) efforts to gain unauthorized access to
5 such a system or network, including to gain
6 such unauthorized access for the purpose of
7 exfiltrating information stored on, processed on,
8 or transiting such a system or network; or

9 “(E) an act of terrorism against an infor-
10 mation system or network of information sys-
11 tems.

12 “(27) The term ‘Federal civilian information
13 systems’—

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

21 “(B) does not include—

22 “(i) a national security system; or

23 “(ii) information, information sys-
24 tems, and networks of information systems
25 that are owned, operated, controlled, or li-

1 censed solely for use by, or on behalf of,
2 the Department of Defense, a military de-
3 partment, or an element of the intelligence
4 community.

5 “(28) The term ‘information security’ means
6 the protection of information, information systems,
7 and networks of information systems from unauthor-
8 ized access, use, disclosure, disruption, modification,
9 or destruction in order to provide—

10 “(A) integrity, including guarding against
11 improper information modification or destruc-
12 tion, including ensuring nonrepudiation and au-
13 thenticity;

14 “(B) confidentiality, including preserving
15 authorized restrictions on access and disclosure,
16 including means for protecting personal privacy
17 and proprietary information; and

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

20 “(29) The term ‘information system’ means the
21 underlying framework and functions used to process,
22 transmit, receive, or store information electronically,
23 including programmable electronic devices, commu-
24 nications networks, and industrial or supervisory

1 control systems and any associated hardware, soft-
2 ware, or data.

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

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

15 **SEC. 102. ENHANCEMENT OF CYBERSECURITY.**

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

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

20 “The Secretary, in collaboration with the heads of
21 other appropriate Federal Government entities, shall con-
22 duct activities for cybersecurity purposes, including the
23 provision of shared situational awareness to each other to
24 enable real-time, integrated, and operational actions to

1 protect from, prevent, mitigate, respond to, and recover
2 from cyber incidents.”.

3 (b) CLERICAL AMENDMENTS.—

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

7 **“Subtitle C—Cybersecurity and**
8 **Information Sharing”.**

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

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

“Sec. 226. Enhancement of cybersecurity.”;

13 and

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

“Subtitle C—Cybersecurity and Information Sharing”.

17 **SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE**
18 **AND INFORMATION SHARING.**

19 (a) IN GENERAL.—Subtitle C of title II of the Home-
20 land Security Act of 2002, as amended by section 102,
21 is further amended by adding at the end the following new
22 section:

1 **“SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE**
2 **AND INFORMATION SHARING.**

3 “(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

4 “(1) IN GENERAL.—The Secretary shall coordi-
5 nate, on an ongoing basis, with Federal, State, and
6 local governments, national laboratories, critical in-
7 frastructure owners, critical infrastructure operators,
8 and other cross sector coordinating entities to—

9 “(A) facilitate a national effort to
10 strengthen and maintain secure, functioning,
11 and resilient critical infrastructure from cyber
12 threats;

13 “(B) ensure that Department policies and
14 procedures enable critical infrastructure owners
15 and critical infrastructure operators to receive
16 real-time, actionable, and relevant cyber threat
17 information;

18 “(C) seek industry sector-specific expertise
19 to—

20 “(i) assist in the development of vol-
21 untary security and resiliency strategies;
22 and

23 “(ii) ensure that the allocation of Fed-
24 eral resources are cost effective and reduce
25 any burden on critical infrastructure own-
26 ers and critical infrastructure operators;

1 “(D) upon request of entities, facilitate
2 and assist risk management efforts of such en-
3 tities to reduce vulnerabilities, identify and dis-
4 rupt threats, and minimize consequences to
5 their critical infrastructure;

6 “(E) upon request of critical infrastructure
7 owners or critical infrastructure operators, pro-
8 vide education and assistance to such owners
9 and operators on how they may use protective
10 measures and countermeasures to strengthen
11 the security and resilience of the Nation’s crit-
12 ical infrastructure; and

13 “(F) coordinate a research and develop-
14 ment strategy to facilitate and promote ad-
15 vancements and innovation in cybersecurity
16 technologies to protect critical infrastructure.

17 “(2) ADDITIONAL RESPONSIBILITIES.—The
18 Secretary shall—

19 “(A) manage Federal efforts to secure,
20 protect, and ensure the resiliency of Federal ci-
21 vilian information systems using a risk-based
22 and performance-based approach, and, upon re-
23 quest of critical infrastructure owners or critical
24 infrastructure operators, support such owners’
25 and operators’ efforts to secure, protect, and

1 ensure the resiliency of critical infrastructure
2 from cyber threats;

3 “(B) direct an entity within the Depart-
4 ment to serve as a Federal civilian entity by
5 and among Federal, State, and local govern-
6 ments, private entities, and critical infrastruc-
7 ture sectors to provide multi-directional sharing
8 of real-time, actionable, and relevant cyber
9 threat information;

10 “(C) build upon existing mechanisms to
11 promote a national awareness effort to educate
12 the general public on the importance of secur-
13 ing information systems;

14 “(D) upon request of Federal, State, and
15 local government entities and private entities,
16 facilitate expeditious cyber incident response
17 and recovery assistance, and provide analysis
18 and warnings related to threats to and
19 vulnerabilities of critical information systems,
20 crisis and consequence management support,
21 and other remote or on-site technical assistance
22 with the heads of other appropriate Federal
23 agencies to Federal, State, and local govern-
24 ment entities and private entities for cyber inci-
25 dents affecting critical infrastructure;

1 “(E) engage with international partners to
2 strengthen the security and resilience of domes-
3 tic critical infrastructure and critical infrastruc-
4 ture located outside of the United States upon
5 which the United States depends; and

6 “(F) conduct outreach to educational insti-
7 tutions, including historically black colleges and
8 universities, Hispanic serving institutions, Na-
9 tive American colleges, and institutions serving
10 persons with disabilities, to encourage such in-
11 stitutions to promote cybersecurity awareness.

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) as appropriate, include relevant
6 small, medium, and large critical infra-
7 structure owners, critical infrastructure op-
8 erators, private entities, and representative
9 trade associations 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 Cybersecu-

1 rity Incident Response Plan in accordance with
2 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 Cyberse-
11 curity and Communications Integration Center es-
12 tablished under section 228(a) of all recognized In-
13 formation Sharing and Analysis Centers under para-
14 graph (1) of this subsection.

15 “(f) CLEARANCES.—The Secretary—

16 “(1) shall expedite the process of security clear-
17 ances under Executive Order No. 13549 or successor
18 orders 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) RECOMMENDATIONS REGARDING NEW AGREE-
2 MENTS.—Not later than 180 days after the date of the
3 enactment of this section, the Secretary shall submit to
4 the appropriate congressional committees recommenda-
5 tions on how to expedite the implementation of informa-
6 tion sharing agreements for cybersecurity purposes be-
7 tween the Secretary and critical information owners and
8 critical infrastructure operators and other private entities.
9 Such recommendations shall address the development and
10 utilization of a scalable form that retains all privacy and
11 other protections in such agreements in existence as of
12 such date, including Cooperative and Research Develop-
13 ment Agreements. Such recommendations should also in-
14 clude any additional authorities or resources that may be
15 needed to carry out the implementation of any such new
16 agreements.

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

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of such Act is amended by adding after
23 the item relating to section 226 (as added by section 102)
24 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 and facilitate discussions with
4 Sector Coordinating Councils, Information Sharing
5 and Analysis Centers, Sector Specific Agencies, and
6 relevant critical infrastructure sectors on the devel-
7 opment of prioritized Federal response efforts, if
8 necessary, to support the defense and recovery of
9 critical infrastructure from cyber incidents;

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 on the development and imple-
14 mentation of procedures to support technology neu-
15 tral real-time information sharing capabilities and
16 mechanisms;

17 “(7) collaborate with the Sector Coordinating
18 Councils, Information Sharing and Analysis Centers,
19 Sector Specific Agencies, and the relevant critical in-
20 frastructure sectors to identify requirements for data
21 and information formats and accessibility, system
22 interoperability, and redundant systems and alter-
23 native capabilities in the event of a disruption in the
24 primary information sharing capabilities and mecha-
25 nisms at the Center;

1 “(8) within the scope of relevant treaties, co-
2 operate with international partners to share infor-
3 mation and respond to cyber incidents;

4 “(9) safeguard sensitive cyber threat informa-
5 tion from unauthorized disclosure;

6 “(10) require other Federal civilian agencies
7 to—

8 “(A) send reports and information to the
9 Center about cyber incidents, threats, and
10 vulnerabilities affecting Federal civilian infor-
11 mation systems and critical infrastructure sys-
12 tems and, in the event a private vendor product
13 or service of such an agency is so implicated,
14 the Center shall first notify such private vendor
15 of the vulnerability before further disclosing
16 such information;

17 “(B) provide to the Center cyber incident
18 detection, analysis, mitigation, and response in-
19 formation; and

20 “(C) immediately send and disclose to the
21 Center cyber threat information received by
22 such agencies;

23 “(11) perform such other duties as the Sec-
24 retary may require to facilitate a national effort to

1 strengthen and maintain secure, functioning, and re-
2 silient critical infrastructure from cyber threats;

3 “(12) implement policies and procedures to—

4 “(A) provide technical assistance to Fed-
5 eral civilian agencies to prevent and respond to
6 data breaches involving unauthorized acquisi-
7 tion or access of personally identifiable informa-
8 tion that occur on Federal civilian information
9 systems;

10 “(B) require Federal civilian agencies to
11 notify the Center about data breaches involving
12 unauthorized acquisition or access of personally
13 identifiable information that occur on Federal
14 civilian information systems without unreason-
15 able delay after the discovery of such a breach;
16 and

17 “(C) require Federal civilian agencies to
18 notify all potential victims of a data breach in-
19 volving unauthorized acquisition or access of
20 personally identifiable information that occur on
21 Federal civilian information systems without
22 unreasonable delay, based on a reasonable de-
23 termination of the level of risk of harm and
24 consistent with the needs of law enforcement;
25 and

1 “(13) participate in exercises run by the De-
2 partment’s National Exercise Program, where ap-
3 propriate.

4 “(e) INTEGRATION AND ANALYSIS.—The Center, in
5 coordination with the Office of Intelligence and Analysis
6 of the Department, shall maintain an integration and
7 analysis function, which shall —

8 “(1) integrate and analyze all cyber threat in-
9 formation received from other Federal agencies,
10 State and local governments, Information Sharing
11 and Analysis Centers, private entities, critical infra-
12 structure owners, and critical infrastructure opera-
13 tors, and share relevant information in near real-
14 time;

15 “(2) on an ongoing basis, assess and evaluate
16 consequence, vulnerability, and threat information to
17 share with the entities referred to in subsection (a)
18 actionable assessments of critical infrastructure sec-
19 tor risks from cyber incidents and to assist critical
20 infrastructure owners and critical infrastructure op-
21 erators by making recommendations to facilitate
22 continuous improvements to the security and resil-
23 iency of the critical infrastructure of the United
24 States;

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

5 “(4) collaborate with the Information Sharing
6 and Analysis Centers to tailor the analysis of infor-
7 mation to the specific characteristics and risk to a
8 relevant critical infrastructure sector; and

9 “(5) assess and evaluate consequence, vulner-
10 ability, and threat information regarding cyber inci-
11 dents in coordination with the Office of Emergency
12 Communications of the Department to help facilitate
13 continuous improvements to the security and resil-
14 iency of public safety communications networks.

15 “(f) REPORT OF CYBER ATTACKS AGAINST FEDERAL
16 GOVERNMENT NETWORKS.—The Secretary shall submit
17 to the Committee on Homeland Security of the House of
18 Representatives, the Committee on Homeland Security
19 and Governmental Affairs of the Senate, and the Comp-
20 troller General of the United States an annual report that
21 summarizes major cyber incidents involving Federal civil-
22 ian agency information systems and provides aggregate
23 statistics on the number of breaches, the extent of any
24 personally identifiable information that was involved, the

1 volume of data exfiltrated, the consequential impact, and
2 the estimated cost of remedying such breaches.

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

11 “(1) the capability and capacity of the Center
12 to carry out its cybersecurity mission in accordance
13 with this section, and sections 226, 227, 229, 230,
14 230A, and 230B;

15 “(2) the extent to which the Department is en-
16 gaged in information sharing with each critical in-
17 frastructure sector designated under section 227(b),
18 including—

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

21 “(B) the extent to which critical infra-
22 structure owners and critical infrastructure op-
23 erators of each critical infrastructure sector
24 participate in information sharing at the Cen-
25 ter;

1 “(3) the volume and range of activities with re-
2 spect to which the Secretary collaborated with the
3 Sector Coordinating Councils and the Sector-Specific
4 Agencies to promote greater engagement with the
5 Center; and

6 “(4) the volume and range of voluntary tech-
7 nical assistance sought and provided by the Depart-
8 ment to each critical infrastructure owner and crit-
9 ical infrastructure operator.”.

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

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

14 (c) GAO REPORT.—Not later than one year after the
15 date of the enactment of this Act, the Comptroller General
16 of the United States shall submit to the Committee on
17 Homeland Security of the House of Representatives and
18 the Committee on Homeland Security and Governmental
19 Affairs of the Senate a report on the effectiveness of the
20 National Cybersecurity and Communications Integration
21 Center established under section 228 of the Homeland Se-
22 curity Act of 2002, as added by subsection (a) of this sec-
23 tion, in carrying out its cybersecurity mission (as such
24 term is defined in section 2 of the Homeland Security Act
25 of 2002, as amended by section 101) in accordance with

1 this Act and such section 228 and sections 226, 227, 229,
2 230, 230A, and 230B of the Homeland Security Act of
3 2002, as added by this Act.

4 **SEC. 105. CYBER INCIDENT RESPONSE AND TECHNICAL AS-**
5 **SISTANCE.**

6 (a) IN GENERAL.—Subtitle C of title II of the Home-
7 land Security Act of 2002, as amended by sections 102,
8 103, and 104, is further amended by adding at the end
9 the following new section:

10 **“SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL**
11 **ASSISTANCE.**

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

14 “(1) upon request, provide timely technical as-
15 sistance and crisis management support to Federal,
16 State, and local government entities, private entities,
17 and critical infrastructure owners and critical infra-
18 structure operators involving cyber incidents affect-
19 ing critical infrastructure; and

20 “(2) upon request, provide actionable rec-
21 ommendations on security and resilience measures
22 and countermeasures to Federal, State, and local
23 government entities, private entities, and critical in-
24 frastructure owners and critical infrastructure oper-
25 ators prior to, during, and after cyber incidents.

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

4 “(c) CYBER INCIDENT RESPONSE PLAN.—The Sec-
5 retary, in coordination with the Sector Coordinating Coun-
6 cils, Information Sharing and Analysis Centers, and Fed-
7 eral, State, and local governments, shall develop, regularly
8 update, maintain, and exercise a National Cybersecurity
9 Incident Response Plan which shall—

10 “(1) include effective emergency response plans
11 associated with cyber threats to critical infrastruc-
12 ture, information systems, or networks of informa-
13 tion systems;

14 “(2) ensure that such National Cybersecurity
15 Incident Response Plan can adapt to and reflect a
16 changing cyber threat environment, and incorporate
17 best practices and lessons learned from regular exer-
18 cises, training, and after-action reports; and

19 “(3) facilitate discussions on the best methods
20 for developing innovative and useful cybersecurity
21 exercises for coordinating between the Department
22 and each of the critical infrastructure sectors des-
23 igned under section 227(b).

24 “(d) UPDATE TO CYBER INCIDENT ANNEX TO THE
25 NATIONAL RESPONSE FRAMEWORK.—The Secretary, in

1 coordination with the heads of other Federal agencies and
2 in accordance with the National Cybersecurity Incident
3 Response Plan under subsection (c), shall regularly up-
4 date, maintain, and exercise the Cyber Incident Annex to
5 the National Response Framework of the Department.”.

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

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

10 **SEC. 106. STREAMLINING OF DEPARTMENT CYBERSECU-**
11 **RITY ORGANIZATION.**

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

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

1 (1) IN GENERAL.—Paragraph (1) of section
2 103(a) of the Homeland Security Act of 2002 (6
3 U.S.C. 113(a)) is amended by adding at the end the
4 following new subparagraphs:

5 “(K) Under Secretary for Cybersecurity
6 and Infrastructure Protection.

7 “(L) Deputy Under Secretary for Cyberse-
8 curity.

9 “(M) Deputy Under Secretary for Infra-
10 structure Protection.”.

11 (2) CONTINUATION IN OFFICE.—The individ-
12 uals who hold the positions referred to in subpara-
13 graphs (K), (L), and (M) of subsection (a) of section
14 103 of the Homeland Security Act of 2002 (as
15 added by paragraph (1) of this subsection) as of the
16 date of the enactment of this Act may continue to
17 hold such positions.

18 (c) REPORT ON IMPROVING THE CAPABILITY AND
19 EFFECTIVENESS OF THE CYBERSECURITY AND COMMU-
20 NICATIONS OFFICE.—To improve the operational capa-
21 bility and effectiveness in carrying out the cybersecurity
22 mission (as such term is defined in section 2 of the Home-
23 land Security Act of 2002, as amended by section 101)
24 of the Department of Homeland Security, the Secretary
25 of Homeland Security shall submit to the Committee on

1 Homeland Security of the House of Representatives and
2 the Committee on Homeland Security and Governmental
3 Affairs of the Senate a report on—

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

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

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

1 of this Act, the Secretary shall submit to the Committee
2 on Homeland Security of the House of Representatives
3 and the Committee on Homeland Security and Govern-
4 mental Affairs of the Senate a report on the effectiveness
5 of the Department's acquisition processes for cybersecu-
6 rity technologies.

7 (e) RESOURCE INFORMATION.—The Secretary of
8 Homeland Security shall make available Department of
9 Homeland Security contact information to serve as a re-
10 source for Sector Coordinating Councils and critical infra-
11 structure owners and critical infrastructure operators to
12 better coordinate cybersecurity efforts with the Depart-
13 ment relating to emergency response and recovery efforts
14 for cyber incidents.

15 **TITLE II—PUBLIC-PRIVATE COL-**
16 **LABORATION ON CYBERSECU-**
17 **RITY**

18 **SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
19 **CURITY.**

20 (a) NATIONAL INSTITUTE OF STANDARDS AND
21 TECHNOLOGY.—

22 (1) IN GENERAL.—The Director of the National
23 Institute of Standards and Technology, in coordina-
24 tion with the Secretary of Homeland Security, shall,
25 on an ongoing basis, facilitate and support the devel-

1 opment of a voluntary, industry-led set of standards,
2 guidelines, best practices, methodologies, procedures,
3 and processes to reduce cyber risks to critical infra-
4 structure. The Director, in coordination with the
5 Secretary—

6 (A) shall—

7 (i) coordinate closely and continuously
8 with relevant private entities, critical infra-
9 structure owners and critical infrastructure
10 operators, Sector Coordinating Councils,
11 Information Sharing and Analysis Centers,
12 and other relevant industry organizations,
13 and incorporate industry expertise to the
14 fullest extent possible;

15 (ii) consult with the Sector Specific
16 Agencies, Federal, State and local govern-
17 ments, the governments of other countries,
18 and international organizations;

19 (iii) utilize a prioritized, flexible, re-
20 peatable, performance-based, and cost-ef-
21 fective approach, including information se-
22 curity measures and controls, that may be
23 voluntarily adopted by critical infrastruc-
24 ture owners and critical infrastructure op-

1 erators to help them identify, assess, and
2 manage cyber risks;

3 (iv) include methodologies to—

4 (I) identify and mitigate impacts
5 of the cybersecurity measures or con-
6 trols on business confidentiality; and

7 (II) protect individual privacy
8 and civil liberties;

9 (v) incorporate voluntary consensus
10 standards and industry best practices, and
11 align with voluntary international stand-
12 ards to the fullest extent possible;

13 (vi) prevent duplication of regulatory
14 processes and prevent conflict with or su-
15 perseding of regulatory requirements, man-
16 datory standards, and processes; and

17 (vii) include such other similar and
18 consistent elements as determined nec-
19 essary; and

20 (B) shall not prescribe or otherwise re-
21 quire—

22 (i) the use of specific solutions;

23 (ii) the use of specific information
24 technology products or services; or

1 (iii) that information technology prod-
2 ucts or services be designed, developed, or
3 manufactured in a particular manner.

4 (2) LIMITATION.—Information shared with or
5 provided to the Director of the National Institute of
6 Standards and Technology or the Secretary of
7 Homeland Security for the purpose of the activities
8 under paragraph (1) may not be used by any Fed-
9 eral, State, or local government department or agen-
10 cy to regulate the activity of any private entity.

11 (b) AMENDMENT.—

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

16 **“SEC. 230. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
17 **CURITY.**

18 “(a) MEETINGS.—The Secretary shall meet with the
19 Sector Coordinating Council for each critical infrastruc-
20 ture sector designated under section 227(b) on a biannual
21 basis to discuss the cybersecurity threat to critical infra-
22 structure, voluntary activities to address cybersecurity,
23 and ideas to improve the public-private partnership to en-
24 hance cybersecurity, in which the Secretary shall—

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

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

9 “(B) the extent and likelihood of death, in-
10 jury, or serious adverse effects to human health
11 and safety caused by an act of terrorism or
12 other disruption, destruction, or unauthorized
13 use of critical infrastructure;

14 “(C) the threat to national security caused
15 by an act of terrorism or other disruption, de-
16 struction, or unauthorized use of critical infra-
17 structure; and

18 “(D) the harm to the economy that would
19 result from an act of terrorism or other disrup-
20 tion, destruction, or unauthorized use of critical
21 infrastructure; and

22 “(2) provide recommendations, which may be
23 voluntarily adopted, on ways to improve cybersecu-
24 rity of critical infrastructure.

25 “(b) REPORT.—

1 “(1) IN GENERAL.—Starting 30 days after the
2 end of the fiscal year in which the National Cyberse-
3 curity and Critical Infrastructure Protection Act of
4 2013 is enacted and annually thereafter, the Sec-
5 retary shall submit to the appropriate congressional
6 committees a report on the state of cybersecurity for
7 each critical infrastructure sector designated under
8 section 227(b) based on discussions between the De-
9 partment and the Sector Coordinating Council in ac-
10 cordance with subsection (a) of this section. The
11 Secretary shall maintain a public copy of each re-
12 port, and each report may include a non-public
13 annex for proprietary, business-sensitive informa-
14 tion, or other sensitive information. Each report
15 shall include, at a minimum information relating
16 to—

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

20 “(B) the extent and nature of any cyberse-
21 curity incidents during the previous year, in-
22 cluding the extent to which cyber incidents
23 jeopardized or imminently jeopardized informa-
24 tion systems;

1 “(C) the current status of the voluntary,
2 industry-led set of standards, guidelines, best
3 practices, methodologies, procedures, and proc-
4 esses to reduce cyber risks within each critical
5 infrastructure sector; and

6 “(D) the volume and range of voluntary
7 technical assistance sought and provided by the
8 Department to each critical infrastructure sec-
9 tor.

10 “(2) SECTOR COORDINATING COUNCIL RE-
11 SPONSE.—Before making public and submitting
12 each report required under paragraph (1), the Sec-
13 retary shall provide a draft of each report to the
14 Sector Coordinating Council for the critical infra-
15 structure sector covered by each such report. The
16 Sector Coordinating Council at issue may provide to
17 the Secretary a written response to such report with-
18 in 45 days of receiving the draft. If such Sector Co-
19 ordinating Council provides a written response, the
20 Secretary shall include such written response in the
21 final version of each report required under para-
22 graph (1).

23 “(c) LIMITATION.—Information shared with or pro-
24 vided to a Sector Coordinating Council, a critical infra-
25 structure sector, or the Secretary for the purpose of the

1 activities under subsections (a) and (b) may not be used
2 by any Federal, State, or local government department or
3 agency to regulate the activity of any private entity.”.

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

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

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

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

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

13 (A) in the heading, by striking “DESIGNA-
14 TION OF QUALIFIED ANTI-TERRORISM TECH-
15 NOLOGIES” and inserting “DESIGNATION OF
16 ANTI-TERRORISM AND CYBERSECURITY TECH-
17 NOLOGIES”;

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

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

24 (D) in paragraph (7)—

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

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

6 (2) in section 863 (6 U.S.C. 442)—

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

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

12 (C) by inserting “or qualifying cyber inci-
13 dents” after “acts of terrorism” each place it
14 appears;

15 (3) in section 864 (6 U.S.C. 443)—

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

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

21 (4) in section 865 (6 U.S.C. 444)—

22 (A) in paragraph (1)—

23 (i) in the heading, by inserting “OR
24 CYBERSECURITY” after “ANTI-TER-
25 RORISM”;

1 (ii) by inserting “or cybersecurity”
2 after “anti-terrorism”;

3 (iii) by inserting “or qualifying cyber
4 incidents” after “acts of terrorism”; and

5 (iv) by inserting “or incidents” after
6 “such acts”; and

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

9 “(7) QUALIFYING CYBER INCIDENT.—

10 “(A) IN GENERAL.—The term ‘qualifying
11 cyber incident’ means any act that the Sec-
12 retary determines meets the requirements under
13 subparagraph (B), as such requirements are
14 further defined and specified by the Secretary.

15 “(B) REQUIREMENTS.—A qualifying cyber
16 incident meets the requirements of this sub-
17 paragraph if—

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

20 “(ii) the incident disrupts or immi-
21 nently jeopardizes the integrity, operation,
22 confidentiality, or availability of program-
23 mable electronic devices, communication
24 networks, including hardware, software
25 and data that are essential to their reliable

1 operation, electronic storage devices, or
2 any other information system, or the infor-
3 mation that system controls, processes,
4 stores, or transmits;

5 “(iii) the perpetrator of the incident
6 gains access to an information system or a
7 network of information systems resulting
8 in—

9 “(I) misappropriation or theft of
10 data, assets, information, or intellec-
11 tual property;

12 “(II) corruption of data, assets,
13 information, or intellectual property;

14 “(III) operational disruption; or

15 “(IV) an adverse effect on such
16 system or network, or the data, as-
17 sets, information, or intellectual prop-
18 erty contained therein; and

19 “(iv) the incident causes harm inside
20 or outside the United States that results in
21 material levels of damage, disruption, or
22 casualties severely affecting the United
23 States population, infrastructure, economy,
24 or national morale, or Federal, State, local,
25 or tribal government functions.

1 “(C) RULE OF CONSTRUCTION.—For pur-
2 poses of clause (iv) of subparagraph (B), the
3 term ‘severely’ includes any qualifying cyber in-
4 cident, whether at a local, regional, state, na-
5 tional, international, or tribal level, that af-
6 fects—

7 “(i) the United States population, in-
8 frastructure, economy, or national morale,
9 or

10 “(ii) Federal, State, local, or tribal
11 government functions.”.

12 (b) FUNDING.—Of the amounts authorized to be ap-
13 propriated for each of fiscal years 2014, 2015, and 2016
14 for the Department of Homeland Security, the Secretary
15 of Homeland Security is authorized to use not less than
16 \$20,000,000 for any such year for the Department’s
17 SAFETY Act Office.

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

19 This Act and the amendments made by this Act (ex-
20 cept that this section shall not apply in the case of section
21 202 of this Act and the amendments made by such section
22 202) do not—

23 (1) create or authorize the issuance of any new
24 regulations or additional Federal Government regu-
25 latory authority; or

1 (2) permit regulatory actions that would dupli-
2 cate, conflict with, or supercede regulatory require-
3 ments, mandatory standards, or related processes.

4 **SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION**
5 **OF APPROPRIATIONS.**

6 No additional funds are authorized to be appro-
7 priated to carry out this Act and the amendments made
8 by this Act. This Act and such amendments shall be car-
9 ried out using amounts otherwise available for such pur-
10 poses.

11 **SEC. 205. PROHIBITION ON COLLECTION ACTIVITIES TO**
12 **TRACK INDIVIDUALS' PERSONALLY IDENTIFI-**
13 **ABLE INFORMATION.**

14 Nothing in this Act shall permit the Department of
15 Homeland Security to engage in the monitoring, surveil-
16 lance, exfiltration, or other collection activities for the pur-
17 pose of tracking an individual's personally identifiable in-
18 formation.

19 **SEC. 206. CYBERSECURITY SCHOLARS.**

20 The Secretary of Homeland Security shall determine
21 the feasibility and potential benefit of developing a visiting
22 security researchers program from academia, including cy-
23 bersecurity scholars at the Department of Homeland Se-
24 curity's Centers of Excellence, as designated by the Sec-
25 retary, to enhance knowledge with respect to the unique

1 challenges of addressing cyber threats to critical infra-
2 structure. Eligible candidates shall possess necessary secu-
3 rity clearances and have a history of working with Federal
4 agencies in matters of national or domestic security.

5 **SEC. 207. NATIONAL RESEARCH COUNCIL STUDY ON THE**
6 **RESILIENCE AND RELIABILITY OF THE NA-**
7 **TION'S POWER GRID.**

8 (a) INDEPENDENT STUDY.—Not later than 60 days
9 after the date of the enactment of this Act, the Secretary
10 of Homeland Security, in coordination with the heads of
11 other departments and agencies, as necessary, shall enter
12 into an agreement with the National Research Council to
13 conduct research of the future resilience and reliability of
14 the Nation's electric power transmission and distribution
15 system. The research under this subsection shall be known
16 as the “Saving More American Resources Today Study”
17 or the “SMART Study”. In conducting such research, the
18 National Research Council shall—

19 (1) research the options for improving the Na-
20 tion's ability to expand and strengthen the capabili-
21 ties of the Nation's power grid, including estimation
22 of the cost, time scale for implementation, and iden-
23 tification of the scale and scope of any potential sig-
24 nificant health and environmental impacts;

1 (2) consider the forces affecting the grid, in-
2 cluding technical, economic, regulatory, environ-
3 mental, and geopolitical factors, and how such forces
4 are likely to affect—

5 (A) the efficiency, control, reliability and
6 robustness of operation;

7 (B) the ability of the grid to recover from
8 disruptions, including natural disasters and ter-
9 rorist attacks;

10 (C) the ability of the grid to incorporate
11 greater reliance on distributed and intermittent
12 power generation and electricity storage;

13 (D) the ability of the grid to adapt to
14 changing patterns of demand for electricity; and

15 (E) the economic and regulatory factors
16 affecting the evolution of the grid;

17 (3) review Federal, State, industry, and aca-
18 demic research and development programs and iden-
19 tify technological options that could improve the fu-
20 ture grid;

21 (4) review studies and analyses prepared by the
22 North American Electric Reliability Corporation
23 (NERC) regarding the future resilience and reli-
24 ability of the grid;

1 (5) review the implications of increased reliance
2 on digital information and control of the power grid
3 for improving reliability, resilience, and congestion
4 and for potentially increasing vulnerability to cyber
5 attack;

6 (6) review regulatory, industry, and institu-
7 tional factors and programs affecting the future of
8 the grid;

9 (7) research the costs and benefits, as well as
10 the strengths and weaknesses, of the options identi-
11 fied under paragraph (1) to address the emerging
12 forces described in paragraph (2) that are shaping
13 the grid;

14 (8) identify the barriers to realizing the options
15 identified and suggest strategies for overcoming
16 those barriers including suggested actions, priorities,
17 incentives, and possible legislative and executive ac-
18 tions; and

19 (9) research the ability of the grid to integrate
20 existing and future infrastructure, including utilities,
21 telecommunications lines, highways, and other crit-
22 ical infrastructure.

23 (b) COOPERATION AND ACCESS TO INFORMATION
24 AND PERSONNEL.—The Secretary shall ensure that the
25 National Research Council receives full and timely co-

1 operation, including full access to information and per-
2 sonnel, from the Department of Homeland Security, the
3 Department of Energy, including the management and op-
4 erating components of the Departments, and other Fed-
5 eral departments and agencies, as necessary, for the pur-
6 poses of conducting the study described in subsection (a).

7 (c) REPORT.—

8 (1) IN GENERAL.—Not later than 18 months
9 from the date on which the Secretary enters into the
10 agreement with the National Research Council de-
11 scribed in subsection (a), the National Research
12 Council shall submit to the Secretary and the Com-
13 mittee on Homeland Security and the Committee on
14 Energy and Commerce of the House of Representa-
15 tives and the Committee on Homeland Security and
16 Governmental Affairs and the Committee on Energy
17 and Natural Resources of the Senate a report con-
18 taining the findings of the research required by that
19 subsection.

20 (2) FORM OF REPORT.—The report under para-
21 graph (1) shall be submitted in unclassified form,
22 but may include a classified annex.

23 (d) FUNDING.—Of the amounts authorized to be ap-
24 propriated for 2014 for the Department of Homeland Se-
25 curity, the Secretary of Homeland Security is authorized

1 to obligate and expend not more than \$2,000,000 for the
 2 National Research Council report.

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 cited as the
 15 ‘Homeland Security Cybersecurity Boots-on-the-Ground
 16 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 cybersecu-
5 rity positions across the Department in a man-
6 ner that allows for tracking of overall recruiting
7 and identifying areas for better coordination
8 and leveraging of resources within the Depart-
9 ment.

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:

“Sec. 230B. Personnel authorities.”.

Passed the House of Representatives July 28, 2014.

Attest:

Clerk.

113TH CONGRESS
2^D SESSION

H. R. 3696

AN ACT

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