

Union Calendar No. 411

113TH CONGRESS
2^D SESSION

H. R. 3696

[Report No. 113–550, Part I]

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

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 11, 2013

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

JULY 23, 2014

Reported from the Committee on Homeland Security with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

JULY 23, 2014

The Committees on Science, Space, and Technology and Oversight and Government Reform discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on December 11, 2013]

A BILL

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,*

3 **SECTION 1. SHORT TITLE.**

4 *This Act may be cited as the “National Cybersecurity*
 5 *and Critical Infrastructure Protection Act of 2014”.*

6 **SEC. 2. TABLE OF CONTENTS.**

7 *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 iden-
tifiable 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.

8 **TITLE I—SECURING THE NATION**
 9 **AGAINST CYBER ATTACK**

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

11 *Section 2 of the Homeland Security Act of 2002 (6*
 12 *U.S.C. 101) is amended by adding at the end the following*
 13 *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 person
8 that manages, runs, or operates, in whole or in part,
9 the day-to-day operations of critical infrastructure.

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

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

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

24 “(C) result in the denial of access to or deg-
25 radation, disruption, or destruction of such a

1 *system or network, or the defeat of an operations*
2 *control or technical control essential to the secu-*
3 *rity or operation of such a system or network.*

4 “(23) *The term ‘cybersecurity mission’ means ac-*
5 *tivities that encompass the full range of threat reduc-*
6 *tion, vulnerability reduction, deterrence, incident re-*
7 *sponse, resiliency, and recovery activities to foster the*
8 *security and stability of cyberspace.*

9 “(24) *The term ‘cybersecurity purpose’ means the*
10 *purpose of ensuring the security, integrity, confiden-*
11 *tiality, or availability of, or safeguarding, an infor-*
12 *mation system or network of information systems, in-*
13 *cluding protecting such a system or network, or data*
14 *residing on such a system or network, including pro-*
15 *tection of such a system or network, from—*

16 “(A) *a vulnerability of such a system or*
17 *network;*

18 “(B) *a threat to the security, integrity, con-*
19 *fidentiality, or availability of such a system or*
20 *network, or any information stored on, processed*
21 *on, or transiting such a system or network;*

22 “(C) *efforts to deny access to or degrade,*
23 *disrupt, or destroy such a system or network; or*

24 “(D) *efforts to gain unauthorized access to*
25 *such a system or network, including to gain such*

1 *unauthorized access for the purpose of*
2 *exfiltrating information stored on, processed on,*
3 *or transiting such a system or network.*

4 “(25) *The term ‘cyber threat’ means any action*
5 *that may result in unauthorized access to, exfiltration*
6 *of, manipulation of, harm of, or impairment to the*
7 *security, integrity, confidentiality, or availability of*
8 *an information system or network of information sys-*
9 *tems, or information that is stored on, processed by,*
10 *or transiting such a system or network.*

11 “(26) *The term ‘cyber threat information’ means*
12 *information directly pertaining to—*

13 “(A) *a vulnerability of an information sys-*
14 *tem or network of information systems of a gov-*
15 *ernment or private entity;*

16 “(B) *a threat to the security, integrity, con-*
17 *fidentiality, or availability of such a system or*
18 *network of a government or private entity, or*
19 *any information stored on, processed on, or*
20 *transiting such a system or network;*

21 “(C) *efforts to deny access to or degrade,*
22 *disrupt, or destroy such a system or network of*
23 *a government or private entity;*

24 “(D) *efforts to gain unauthorized access to*
25 *such a system or network, including to gain such*

1 *unauthorized access for the purpose of*
2 *exfiltrating information stored on, processed on,*
3 *or transiting such a system or network; or*

4 *“(E) an act of terrorism against an infor-*
5 *mation system or network of information sys-*
6 *tems.*

7 *“(27) The term ‘Federal civilian information*
8 *systems’—*

9 *“(A) means information, information sys-*
10 *tems, and networks of information systems that*
11 *are owned, operated, controlled, or licensed for*
12 *use by, or on behalf of, any Federal agency, in-*
13 *cluding such systems or networks used or oper-*
14 *ated by another entity on behalf of a Federal*
15 *agency; but*

16 *“(B) does not include—*

17 *“(i) a national security system; or*

18 *“(ii) information, information systems,*
19 *and networks of information systems that*
20 *are owned, operated, controlled, or licensed*
21 *solely for use by, or on behalf of, the De-*
22 *partment of Defense, a military depart-*
23 *ment, or an element of the intelligence com-*
24 *munity.*

1 “(28) *The term ‘information security’ means the*
2 *protection of information, information systems, and*
3 *networks of information systems from unauthorized*
4 *access, use, disclosure, disruption, modification, or de-*
5 *struction in order to provide—*

6 “(A) *integrity, including guarding against*
7 *improper information modification or destruc-*
8 *tion, including ensuring nonrepudiation and au-*
9 *thenticity;*

10 “(B) *confidentiality, including preserving*
11 *authorized restrictions on access and disclosure,*
12 *including means for protecting personal privacy*
13 *and proprietary information; and*

14 “(C) *availability, including ensuring timely*
15 *and reliable access to and use of information.*

16 “(29) *The term ‘information system’ means the*
17 *underlying framework and functions used to process,*
18 *transmit, receive, or store information electronically,*
19 *including programmable electronic devices, commu-*
20 *nications networks, and industrial or supervisory*
21 *control systems and any associated hardware, soft-*
22 *ware, or data.*

23 “(30) *The term ‘private entity’ means any indi-*
24 *vidual or any private or publically-traded company,*
25 *public or private utility (including a utility that is*

1 *a unit of a State or local government, or a political*
2 *subdivision of a State government), organization, or*
3 *corporation, including an officer, employee, or agent*
4 *thereof.*

5 *“(31) The term ‘shared situational awareness’*
6 *means an environment in which cyber threat infor-*
7 *mation is shared in real time between all designated*
8 *Federal cyber operations centers to provide actionable*
9 *information about all known cyber threats.”.*

10 **SEC. 102. ENHANCEMENT OF CYBERSECURITY.**

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

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

15 *“The Secretary, in collaboration with the heads of*
16 *other appropriate Federal Government entities, shall con-*
17 *duct activities for cybersecurity purposes, including the pro-*
18 *vision of shared situational awareness to each other to en-*
19 *able real-time, integrated, and operational actions to pro-*
20 *tect from, prevent, mitigate, respond to, and recover from*
21 *cyber incidents.”.*

22 *(b) CLERICAL AMENDMENTS.—*

23 *(1) SUBTITLE HEADING.—The heading for sub-*
24 *title C of title II of such Act is amended to read as*
25 *follows:*

1 **“Subtitle C—Cybersecurity and**
 2 **Information Sharing”.**

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

5 (A) *by adding after the item relating to sec-*
 6 *tion 225 the following new item:*

 “*Sec. 226. Enhancement of cybersecurity.*”;

7 *and*

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

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

11 **SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE**
 12 **AND INFORMATION SHARING.**

13 (a) *IN GENERAL.*—*Subtitle C of title II of the Home-*
 14 *land Security Act of 2002, as amended by section 102, is*
 15 *further amended by adding at the end the following new*
 16 *section:*

17 **“SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE**
 18 **AND INFORMATION SHARING.**

19 “(a) *PROTECTION OF CRITICAL INFRASTRUCTURE.*—

20 “(1) *IN GENERAL.*—*The Secretary shall coordi-*
 21 *nate, on an ongoing basis, with Federal, State, and*
 22 *local governments, national laboratories, critical in-*
 23 *frastructure owners, critical infrastructure operators,*
 24 *and other cross sector coordinating entities to—*

1 “(A) facilitate a national effort to strength-
2 en and maintain secure, functioning, and resil-
3 ient critical infrastructure from cyber threats;

4 “(B) ensure that Department policies and
5 procedures enable critical infrastructure owners
6 and critical infrastructure operators to receive
7 real-time, actionable, and relevant cyber threat
8 information;

9 “(C) seek industry sector-specific expertise
10 to—

11 “(i) assist in the development of vol-
12 untary security and resiliency strategies;
13 and

14 “(ii) ensure that the allocation of Fed-
15 eral resources are cost effective and reduce
16 any burden on critical infrastructure own-
17 ers and critical infrastructure operators;

18 “(D) upon request of entities, facilitate and
19 assist risk management efforts of such entities to
20 reduce vulnerabilities, identify and disrupt
21 threats, and minimize consequences to their crit-
22 ical infrastructure;

23 “(E) upon request of critical infrastructure
24 owners or critical infrastructure operators, pro-
25 vide education and assistance to such owners

1 *and operators on how they may use protective*
2 *measures and countermeasures to strengthen the*
3 *security and resilience of the Nation’s critical in-*
4 *frastructure; and*

5 *“(F) coordinate a research and development*
6 *strategy to facilitate and promote advancements*
7 *and innovation in cybersecurity technologies to*
8 *protect critical infrastructure.*

9 *“(2) ADDITIONAL RESPONSIBILITIES.—The Sec-*
10 *retary shall—*

11 *“(A) manage Federal efforts to secure, pro-*
12 *tect, and ensure the resiliency of Federal civilian*
13 *information systems using a risk-based and per-*
14 *formance-based approach, and, upon request of*
15 *critical infrastructure owners or critical infra-*
16 *structure operators, support such owners’ and*
17 *operators’ efforts to secure, protect, and ensure*
18 *the resiliency of critical infrastructure from*
19 *cyber threats;*

20 *“(B) direct an entity within the Depart-*
21 *ment to serve as a Federal civilian entity by and*
22 *among Federal, State, and local governments,*
23 *private entities, and critical infrastructure sec-*
24 *tors to provide multi-directional sharing of real-*

1 *time, actionable, and relevant cyber threat infor-*
2 *mation;*

3 “(C) *build upon existing mechanisms to*
4 *promote a national awareness effort to educate*
5 *the general public on the importance of securing*
6 *information systems;*

7 “(D) *upon request of Federal, State, and*
8 *local government entities and private entities, fa-*
9 *facilitate expeditious cyber incident response and*
10 *recovery assistance, and provide analysis and*
11 *warnings related to threats to and vulnerabilities*
12 *of critical information systems, crisis and con-*
13 *sequence management support, and other remote*
14 *or on-site technical assistance with the heads of*
15 *other appropriate Federal agencies to Federal,*
16 *State, and local government entities and private*
17 *entities for cyber incidents affecting critical in-*
18 *frastructure;*

19 “(E) *engage with international partners to*
20 *strengthen the security and resilience of domestic*
21 *critical infrastructure and critical infrastructure*
22 *located outside of the United States upon which*
23 *the United States depends; and*

24 “(F) *conduct outreach to educational insti-*
25 *tutions, including historically black colleges and*

1 *universities, Hispanic serving institutions, Na-*
2 *tive American colleges, and institutions serving*
3 *persons with disabilities, to encourage such insti-*
4 *tutions to promote cybersecurity awareness.*

5 “(3) *RULE OF CONSTRUCTION.*—*Nothing in this*
6 *section may be construed to require any private enti-*
7 *ty to request assistance from the Secretary, or require*
8 *any private entity requesting such assistance to im-*
9 *plement any measure or recommendation suggested by*
10 *the Secretary.*

11 “(b) *CRITICAL INFRASTRUCTURE SECTORS.*—*The Sec-*
12 *retary, in collaboration with the heads of other appropriate*
13 *Federal agencies, shall designate critical infrastructure sec-*
14 *tors (that may include subdivisions of sectors within a sec-*
15 *tor as the Secretary may determine appropriate). The crit-*
16 *ical infrastructure sectors designated under this subsection*
17 *may include the following:*

18 “(1) *Chemical.*

19 “(2) *Commercial facilities.*

20 “(3) *Communications.*

21 “(4) *Critical manufacturing.*

22 “(5) *Dams.*

23 “(6) *Defense Industrial Base.*

24 “(7) *Emergency services.*

25 “(8) *Energy.*

1 “(9) *Financial services.*

2 “(10) *Food and agriculture.*

3 “(11) *Government facilities.*

4 “(12) *Healthcare and public health.*

5 “(13) *Information technology.*

6 “(14) *Nuclear reactors, materials, and waste.*

7 “(15) *Transportation systems.*

8 “(16) *Water and wastewater systems.*

9 “(17) *Such other sectors as the Secretary deter-*
10 *mines appropriate.*

11 “(c) *SECTOR SPECIFIC AGENCIES.—The Secretary, in*
12 *collaboration with the relevant critical infrastructure sector*
13 *and the heads of other appropriate Federal agencies, shall*
14 *recognize the Federal agency designated as of November 1,*
15 *2013, as the ‘Sector Specific Agency’ for each critical infra-*
16 *structure sector designated under subsection (b). If the des-*
17 *ignated Sector Specific Agency for a particular critical in-*
18 *frastructure sector is the Department, for the purposes of*
19 *this section, the Secretary shall carry out this section. The*
20 *Secretary, in coordination with the heads of each such Sec-*
21 *tor Specific Agency shall—*

22 “(1) *support the security and resilience activities*
23 *of the relevant critical infrastructure sector in accord-*
24 *ance with this subtitle; and*

1 “(2) *provide institutional knowledge and special-*
2 *ized expertise to the relevant critical infrastructure*
3 *sector.*

4 “(d) *SECTOR COORDINATING COUNCILS.—*

5 “(1) *RECOGNITION.—The Secretary, in collabo-*
6 *ration with each critical infrastructure sector and the*
7 *relevant Sector Specific Agency, shall recognize and*
8 *partner with the Sector Coordinating Council for*
9 *each critical infrastructure sector designated under*
10 *subsection (b) to coordinate with each such sector on*
11 *security and resilience activities and emergency re-*
12 *sponse and recovery efforts.*

13 “(2) *MEMBERSHIP.—*

14 “(A) *IN GENERAL.—The Sector Coordi-*
15 *nating Council for a critical infrastructure sec-*
16 *tor designated under subsection (b) shall—*

17 “(i) *be comprised exclusively of rel-*
18 *evant critical infrastructure owners, critical*
19 *infrastructure operators, private entities,*
20 *and representative trade associations for the*
21 *sector;*

22 “(ii) *reflect the unique composition of*
23 *each sector; and*

24 “(iii) *include relevant small, medium,*
25 *and large critical infrastructure owners,*

1 *critical infrastructure operators, private en-*
2 *tities, and representative trade associations*
3 *for the sector.*

4 “(B) *PROHIBITION.*—*No government entity*
5 *with regulating authority shall be a member of*
6 *the Sector Coordinating Council.*

7 “(C) *LIMITATION.*—*The Secretary shall*
8 *have no role in the determination of the member-*
9 *ship of a Sector Coordinating Council.*

10 “(3) *ROLES AND RESPONSIBILITIES.*—*The Sector*
11 *Coordinating Council for a critical infrastructure sec-*
12 *tor shall—*

13 “(A) *serve as a self-governing, self-organized*
14 *primary policy, planning, and strategic commu-*
15 *nications entity for coordinating with the De-*
16 *partment, the relevant Sector-Specific Agency*
17 *designated under subsection (c), and the relevant*
18 *Information Sharing and Analysis Centers*
19 *under subsection (e) on security and resilience*
20 *activities and emergency response and recovery*
21 *efforts;*

22 “(B) *establish governance and operating*
23 *procedures, and designate a chairperson for the*
24 *sector to carry out the activities described in this*
25 *subsection;*

1 “(C) coordinate with the Department, the
2 relevant Information Sharing and Analysis Cen-
3 ters under subsection (e), and other Sector Co-
4 ordinating Councils to update, maintain, and
5 exercise the National Cybersecurity Incident Re-
6 sponse Plan in accordance with section 229(b);
7 and

8 “(D) provide any recommendations to the
9 Department on infrastructure protection tech-
10 nology gaps to help inform research and develop-
11 ment efforts at the Department.

12 “(e) *SECTOR INFORMATION SHARING AND ANALYSIS*
13 *CENTERS.*—

14 “(1) *RECOGNITION.*—*The Secretary, in collabo-*
15 *ration with the relevant Sector Coordinating Council*
16 *and the critical infrastructure sector represented by*
17 *such Council, and in coordination with the relevant*
18 *Sector Specific Agency, shall recognize at least one*
19 *Information Sharing and Analysis Center for each*
20 *critical infrastructure sector designated under sub-*
21 *section (b) for purposes of paragraph (3). No other*
22 *Information Sharing and Analysis Organizations, in-*
23 *cluding Information Sharing and Analysis Centers,*
24 *may be precluded from having an information shar-*
25 *ing relationship within the National Cybersecurity*

1 *and Communications Integration Center established*
2 *pursuant to section 228. Nothing in this subsection or*
3 *any other provision of this subtitle may be construed*
4 *to limit, restrict, or condition any private entity or*
5 *activity utilized by, among, or between private enti-*
6 *ties.*

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

11 “(A) *serve as an information sharing re-*
12 *source for such sector and promote ongoing*
13 *multi-directional sharing of real-time, relevant,*
14 *and actionable cyber threat information and*
15 *analysis by and among such sector, the Depart-*
16 *ment, the relevant Sector Specific Agency, and*
17 *other critical infrastructure sector Information*
18 *Sharing and Analysis Centers;*

19 “(B) *establish governance and operating*
20 *procedures to carry out the activities conducted*
21 *under this subsection;*

22 “(C) *serve as an emergency response and re-*
23 *covery operations coordination point for such*
24 *sector, and upon request, facilitate cyber incident*
25 *response capabilities in coordination with the*

1 *Department, the relevant Sector Specific Agency*
2 *and the relevant Sector Coordinating Council;*

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

7 *“(E) coordinate with the Department, the*
8 *relevant Sector Coordinating Council, the rel-*
9 *evant Sector Specific Agency, and other critical*
10 *infrastructure sector Information Sharing and*
11 *Analysis Centers on the development, integra-*
12 *tion, and implementation of procedures to sup-*
13 *port technology neutral, real-time information*
14 *sharing capabilities and mechanisms within the*
15 *National Cybersecurity and Communications In-*
16 *tegration Center established pursuant to section*
17 *228, including—*

18 *“(i) the establishment of a mechanism*
19 *to voluntarily report identified*
20 *vulnerabilities and opportunities for im-*
21 *provement;*

22 *“(ii) the establishment of metrics to as-*
23 *sess the effectiveness and timeliness of the*
24 *Department’s and Information Sharing and*

1 *Analysis Centers’ information sharing ca-*
2 *pabilities; and*

3 *“(iii) the establishment of a mecha-*
4 *nism for anonymous suggestions and com-*
5 *ments;*

6 *“(F) implement an integration and anal-*
7 *ysis function to inform sector planning, risk*
8 *mitigation, and operational activities regarding*
9 *the protection of each critical infrastructure sec-*
10 *tor from cyber incidents;*

11 *“(G) combine consequence, vulnerability,*
12 *and threat information to share actionable as-*
13 *sessments of critical infrastructure sector risks*
14 *from cyber incidents;*

15 *“(H) coordinate with the Department, the*
16 *relevant Sector Specific Agency, and the relevant*
17 *Sector Coordinating Council to update, main-*
18 *tain, and exercise the National Cybersecurity In-*
19 *cident Response Plan in accordance with section*
20 *229(b); and*

21 *“(I) safeguard cyber threat information*
22 *from unauthorized disclosure.*

23 *“(3) FUNDING.—Of the amounts authorized to be*
24 *appropriated for each of fiscal years 2014, 2015, and*
25 *2016 for the Cybersecurity and Communications Of-*

1 *office of the Department, the Secretary is authorized to*
2 *use not less than \$25,000,000 for any such year for*
3 *operations support at the National Cybersecurity and*
4 *Communications Integration Center established under*
5 *section 228(a) of all recognized Information Sharing*
6 *and Analysis Centers under paragraph (1) of this*
7 *subsection.*

8 *“(f) CLEARANCES.—The Secretary—*

9 *“(1) shall expedite the process of security clear-*
10 *ances under Executive Order 13549 or successor or-*
11 *ders for appropriate representatives of Sector Coordi-*
12 *nating Councils and the critical infrastructure sector*
13 *Information Sharing and Analysis Centers; and*

14 *“(2) may so expedite such processing to—*

15 *“(A) appropriate personnel of critical infra-*
16 *structure owners and critical infrastructure op-*
17 *erators; and*

18 *“(B) any other person as determined by the*
19 *Secretary.*

20 *“(g) PUBLIC-PRIVATE COLLABORATION.—The Sec-*
21 *retary, in collaboration with the critical infrastructure sec-*
22 *tors designated under subsection (b), such sectors’ Sector*
23 *Specific Agencies recognized under subsection (c), and the*
24 *Sector Coordinating Councils recognized under subsection*
25 *(d), shall—*

1 “(1) *conduct an analysis and review of the exist-*
2 *ing public-private partnership model and evaluate*
3 *how the model between the Department and critical*
4 *infrastructure owners and critical infrastructure op-*
5 *erators can be improved to ensure the Department,*
6 *critical infrastructure owners, and critical infrastruc-*
7 *ture operators are equal partners and regularly col-*
8 *laborate on all programs and activities of the Depart-*
9 *ment to protect critical infrastructure;*

10 “(2) *develop and implement procedures to ensure*
11 *continuous, collaborative, and effective interactions*
12 *between the Department, critical infrastructure own-*
13 *ers, and critical infrastructure operators; and*

14 “(3) *ensure critical infrastructure sectors have a*
15 *reasonable period for review and comment of all joint-*
16 *ly produced materials with the Department.*

17 “(h) *PROTECTION OF FEDERAL CIVILIAN INFORMA-*
18 *TION SYSTEMS.—*

19 “(1) *IN GENERAL.—The Secretary shall admin-*
20 *ister the operational information security activities*
21 *and functions to protect and ensure the resiliency of*
22 *all Federal civilian information systems.*

23 “(2) *ROLES AND RESPONSIBILITIES.—The Sec-*
24 *retary, in coordination with the heads of other Fed-*
25 *eral civilian agencies, shall—*

1 “(A) develop, issue, and oversee the imple-
2 mentation and compliance of all operational in-
3 formation security policies and procedures to
4 protect and ensure the resiliency of Federal civil-
5 ian information systems;

6 “(B) administer Federal Government-wide
7 efforts to develop and provide adequate, risk-
8 based, cost-effective, and technology neutral in-
9 formation security capabilities;

10 “(C) establish and sustain continuous
11 diagnostics systems for Federal civilian informa-
12 tion systems to aggregate data and identify and
13 prioritize the mitigation of cyber vulnerabilities
14 in such systems for cybersecurity purposes;

15 “(D) develop, acquire, and operate an inte-
16 grated and consolidated system of intrusion de-
17 tection, analytics, intrusion prevention, and
18 other information sharing and protective capa-
19 bilities to defend Federal civilian information
20 systems from cyber threats;

21 “(E) develop and conduct targeted risk as-
22 sessments and operational evaluations of Federal
23 civilian information systems, in consultation
24 with government and private entities that own
25 and operate such information systems, including

1 *threat, vulnerability, and impact assessments*
2 *and penetration testing;*

3 “(F) *develop and provide technical assist-*
4 *ance and cyber incident response capabilities to*
5 *secure and ensure the resilience of Federal civil-*
6 *ian information systems;*

7 “(G) *review annually the operational infor-*
8 *mation security activities and functions of each*
9 *of the Federal civilian agencies;*

10 “(H) *develop minimum technology neutral*
11 *operational requirements for network and secu-*
12 *rity operations centers to facilitate the protection*
13 *of all Federal civilian information systems;*

14 “(I) *develop reporting requirements, con-*
15 *sistent with relevant law, to ensure the National*
16 *Cybersecurity and Communications Integration*
17 *Center established pursuant to section 228 re-*
18 *ceives all actionable cyber threat information*
19 *identified on Federal civilian information sys-*
20 *tems;*

21 “(J) *develop technology neutral performance*
22 *requirements and metrics for the security of Fed-*
23 *eral civilian information systems;*

24 “(K) *implement training requirements that*
25 *include industry recognized certifications to en-*

1 *sure that Federal civilian agencies are able to*
2 *fully and timely comply with policies and proce-*
3 *dures issued by the Secretary under this sub-*
4 *section; and*

5 *“(L) develop training requirements regard-*
6 *ing privacy, civil rights, civil liberties, and in-*
7 *formation oversight for information security em-*
8 *ployees who operate Federal civilian information*
9 *systems.*

10 *“(3) USE OF CERTAIN COMMUNICATIONS.—*

11 *“(A) IN GENERAL.—The Secretary may*
12 *enter into contracts or other agreements, or oth-*
13 *erwise request and obtain, in accordance with*
14 *applicable law, the assistance of private entities*
15 *that provide electronic communication services,*
16 *remote computing services, or cybersecurity serv-*
17 *ices to acquire, intercept, retain, use, and dis-*
18 *close communications and other system traffic,*
19 *deploy countermeasures, or otherwise operate*
20 *protective capabilities in accordance with sub-*
21 *paragraphs (C), (D), (E), and (F) of paragraph*
22 *(2). No cause of action shall exist against private*
23 *entities for assistance provided to the Secretary*
24 *in accordance with this subsection.*

1 “(B) *RULE OF CONSTRUCTION.*—*Nothing in*
2 *subparagraph (A) may be construed to—*

3 “*(i) require or compel any private en-*
4 *tity to enter in a contract or agreement de-*
5 *scribed in such subparagraph; or*

6 “*(ii) authorize the Secretary to take*
7 *any action with respect to any communica-*
8 *tions or system traffic transiting or residing*
9 *on any information system or network of*
10 *information systems other than a Federal*
11 *civilian information system.*

12 “(i) *RECOMMENDATIONS REGARDING NEW AGREE-*
13 *MENTS.*—*Not later than 180 days after the date of the en-*
14 *actment of this section, the Secretary shall submit to the*
15 *appropriate congressional committees recommendations on*
16 *how to expedite the implementation of information sharing*
17 *agreements for cybersecurity purposes between the Secretary*
18 *and critical information owners and critical infrastructure*
19 *operators and other private entities. Such recommendations*
20 *shall address the development and utilization of a scalable*
21 *form that retains all privacy and other protections in such*
22 *agreements in existence as of such date, including Coopera-*
23 *tive and Research Development Agreements. Such rec-*
24 *ommendations should also include any additional authori-*

1 *ties or resources that may be needed to carry out the imple-*
 2 *mentation of any such new agreements.*

3 “(j) *RULE OF CONSTRUCTION.*—*No provision of this*
 4 *title may be construed as modifying, limiting, or otherwise*
 5 *affecting the authority of any other Federal agency under*
 6 *any other provision of law.”.*

7 (b) *CLERICAL AMENDMENT.*—*The table of contents in*
 8 *section 1(b) of such Act is amended by adding after the item*
 9 *relating to section 226 (as added by section 102) the fol-*
 10 *lowing new item:*

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

11 **SEC. 104. NATIONAL CYBERSECURITY AND COMMUNICA-**
 12 **TIONS INTEGRATION CENTER.**

13 (a) *IN GENERAL.*—*Subtitle C of title II of the Home-*
 14 *land Security Act of 2002, as amended by sections 102 and*
 15 *103, is further amended by adding at the end the following*
 16 *new section:*

17 **“SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICA-**
 18 **TIONS INTEGRATION CENTER.**

19 “(a) *ESTABLISHMENT.*—*There is established in the De-*
 20 *partment the National Cybersecurity and Communications*
 21 *Integration Center (referred to in this section as the ‘Cen-*
 22 *ter’), which shall be a Federal civilian information sharing*
 23 *interface that provides shared situational awareness to en-*
 24 *able real-time, integrated, and operational actions across*
 25 *the Federal Government, and share cyber threat informa-*

1 *tion by and among Federal, State, and local government*
2 *entities, Information Sharing and Analysis Centers, private*
3 *entities, and critical infrastructure owners and critical in-*
4 *frastructure operators that have an information sharing re-*
5 *lationship with the Center.*

6 “(b) *COMPOSITION.—The Center shall include each of*
7 *the following entities:*

8 “(1) *At least one Information Sharing and Anal-*
9 *ysis Center established under section 227(e) for each*
10 *critical infrastructure sector.*

11 “(2) *The Multi-State Information Sharing and*
12 *Analysis Center to collaborate with State and local*
13 *governments.*

14 “(3) *The United States Computer Emergency*
15 *Readiness Team to coordinate cyber threat informa-*
16 *tion sharing, proactively manage cyber risks to the*
17 *United States, collaboratively respond to cyber inci-*
18 *dents, provide technical assistance to information sys-*
19 *tem owners and operators, and disseminate timely*
20 *notifications regarding current and potential cyber*
21 *threats and vulnerabilities.*

22 “(4) *The Industrial Control System Cyber Emer-*
23 *gency Response Team to coordinate with industrial*
24 *control systems owners and operators and share in-*

1 *dustrial control systems-related security incidents and*
2 *mitigation measures.*

3 “(5) *The National Coordinating Center for Tele-*
4 *communications to coordinate the protection, re-*
5 *sponse, and recovery of national security emergency*
6 *communications.*

7 “(6) *Such other Federal, State, and local govern-*
8 *ment entities, private entities, organizations, or indi-*
9 *viduals as the Secretary may consider appropriate*
10 *that agree to be included.*

11 “(c) *CYBER INCIDENT.—In the event of a cyber inci-*
12 *dent, the Secretary may grant the entities referred to in*
13 *subsection (a) immediate temporary access to the Center as*
14 *a situation may warrant.*

15 “(d) *ROLES AND RESPONSIBILITIES.—The Center*
16 *shall—*

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

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

4 “(3) provide, upon request, timely technical as-
5 sistance and crisis management support to Federal,
6 State, and local government entities and private enti-
7 ties that own or operate information systems or net-
8 works of information systems to protect from, prevent,
9 mitigate, respond to, and recover from cyber inci-
10 dents;

11 “(4) facilitate cross-sector coordination and shar-
12 ing of cyber threat information to prevent related or
13 consequential impacts to other critical infrastructure
14 sectors;

15 “(5) collaborate and facilitate discussions with
16 Sector Coordinating Councils, Information Sharing
17 and Analysis Centers, Sector Specific Agencies, and
18 relevant critical infrastructure sectors on the develop-
19 ment of prioritized Federal response efforts, if nec-
20 essary, to support the defense and recovery of critical
21 infrastructure from cyber incidents;

22 “(6) collaborate with the Sector Coordinating
23 Councils, Information Sharing and Analysis Centers,
24 Sector Specific Agencies, and the relevant critical in-
25 frastructure sectors on the development and imple-

1 *mentation of procedures to support technology neutral*
2 *real-time information sharing capabilities and mech-*
3 *anisms;*

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

13 *“(8) within the scope of relevant treaties, cooper-*
14 *ate with international partners to share information*
15 *and respond to cyber incidents;*

16 *“(9) safeguard sensitive cyber threat information*
17 *from unauthorized disclosure;*

18 *“(10) require other Federal civilian agencies*
19 *to—*

20 *“(A) send reports and information to the*
21 *Center about cyber incidents, threats, and*
22 *vulnerabilities affecting Federal civilian infor-*
23 *mation systems and critical infrastructure sys-*
24 *tems and, in the event a private vendor product*
25 *or service of such an agency is so implicated, the*

1 Center shall first notify such private vendor of
2 the vulnerability before further disclosing such
3 information;

4 “(B) provide to the Center cyber incident
5 detection, analysis, mitigation, and response in-
6 formation; and

7 “(C) immediately send and disclose to the
8 Center cyber threat information received by such
9 agencies;

10 “(11) perform such other duties as the Secretary
11 may require to facilitate a national effort to strength-
12 en and maintain secure, functioning, and resilient
13 critical infrastructure from cyber threats;

14 “(12) implement policies and procedures to—

15 “(A) provide technical assistance to Federal
16 civilian agencies to prevent and respond to data
17 breaches involving unauthorized acquisition or
18 access of personally identifiable information that
19 occur on Federal civilian information systems;

20 “(B) require Federal civilian agencies to
21 notify the Center about data breaches involving
22 unauthorized acquisition or access of personally
23 identifiable information that occur on Federal
24 civilian information systems not later than two

1 *business days after the discovery of such a*
2 *breach; and*

3 “(C) *require Federal civilian agencies to no-*
4 *tify all potential victims of a data breach involv-*
5 *ing unauthorized acquisition or access of person-*
6 *ally identifiable information that occur on Fed-*
7 *eral civilian information systems without unrea-*
8 *sonable delay consistent with the needs of law en-*
9 *forcement; and*

10 “(13) *participate in exercises run by the Depart-*
11 *ment’s National Exercise Program, where appro-*
12 *priate.*

13 “(e) *INTEGRATION AND ANALYSIS.—The Center, in co-*
14 *ordination with the Office of Intelligence and Analysis of*
15 *the Department, shall maintain an integration and anal-*
16 *ysis function, which shall —*

17 “(1) *integrate and analyze all cyber threat infor-*
18 *mation received from other Federal agencies, State*
19 *and local governments, Information Sharing and*
20 *Analysis Centers, private entities, critical infrastruc-*
21 *ture owners, and critical infrastructure operators,*
22 *and share relevant information in near real-time;*

23 “(2) *on an ongoing basis, assess and evaluate*
24 *consequence, vulnerability, and threat information to*
25 *share with the entities referred to in subsection (a) ac-*

1 *tionable assessments of critical infrastructure sector*
2 *risks from cyber incidents and to assist critical infra-*
3 *structure owners and critical infrastructure operators*
4 *by making recommendations to facilitate continuous*
5 *improvements to the security and resiliency of the*
6 *critical infrastructure of the United States;*

7 *“(3) facilitate cross-sector integration, identifica-*
8 *tion, and analysis of key interdependencies to prevent*
9 *related or consequential impacts to other critical in-*
10 *frastructure sectors;*

11 *“(4) collaborate with the Information Sharing*
12 *and Analysis Centers to tailor the analysis of infor-*
13 *mation to the specific characteristics and risk to a*
14 *relevant critical infrastructure sector; and*

15 *“(5) assess and evaluate consequence, vulner-*
16 *ability, and threat information regarding cyber inci-*
17 *dents in coordination with the Office of Emergency*
18 *Communications of the Department to help facilitate*
19 *continuous improvements to the security and resil-*
20 *ency of public safety communications networks.*

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

1 *General of the United States an annual report that summa-*
2 *rizes major cyber incidents involving Federal civilian agen-*
3 *cy information systems and provides aggregate statistics on*
4 *the number of breaches, the extent of any personally identi-*
5 *fiable information that was involved, the volume of data*
6 *exfiltrated, the consequential impact, and the estimated cost*
7 *of remedying such breaches.*

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

16 “(1) *the capability and capacity of the Center to*
17 *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 infrastruc-
2 ture owners and critical infrastructure operators
3 of each critical infrastructure sector participate
4 in information sharing at the Center;

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

10 “(4) the volume and range of voluntary technical
11 assistance sought and provided by the Department to
12 each critical infrastructure owner and critical infra-
13 structure operator.”.

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

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

18 (c) *GAO REPORT.*—Not later than one year after the
19 date of the enactment of this Act, the Comptroller General
20 of the United States shall submit to the Committee on
21 Homeland Security of the House of Representatives and the
22 Committee on Homeland Security and Governmental Af-
23 fairs of the Senate a report on the effectiveness of the Na-
24 tional Cybersecurity and Communications Integration Cen-
25 ter established under section 228 of the Homeland Security

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

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

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

14 **“SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL AS-**
15 **SISTANCE.**

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

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

24 *“(2) upon request, provide actionable rec-*
25 *ommendations on security and resilience measures*

1 *and countermeasures to Federal, State, and local gov-*
2 *ernment entities, private entities, and critical infra-*
3 *structure owners and critical infrastructure operators*
4 *prior to, during, and after cyber incidents.*

5 “(b) *COORDINATION.*—*In carrying out subsection (a),*
6 *the Secretary shall coordinate with the relevant Sector Spe-*
7 *cific Agencies, if applicable.*

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

14 “(1) *include effective emergency response plans*
15 *associated with cyber threats to critical infrastruc-*
16 *ture, information systems, or networks of information*
17 *systems;*

18 “(2) *ensure that such National Cybersecurity In-*
19 *cident Response Plan can adapt to and reflect a*
20 *changing cyber threat environment, and incorporate*
21 *best practices and lessons learned from regular exer-*
22 *cises, training, and after-action reports; and*

23 “(3) *facilitate discussions on the best methods for*
24 *developing innovative and useful cybersecurity exer-*
25 *cises for coordinating between the Department and*

1 *each of the critical infrastructure sectors designated*
2 *under section 227(b).*

3 “(d) *UPDATE TO CYBER INCIDENT ANNEX TO THE NA-*
4 *TIONAL RESPONSE FRAMEWORK.—The Secretary, in co-*
5 *ordination with the heads of other Federal agencies and in*
6 *accordance with the National Cybersecurity Incident Re-*
7 *sponse Plan under subsection (c), shall regularly update,*
8 *maintain, and exercise the Cyber Incident Annex to the Na-*
9 *tional Response Framework of the Department.”.*

10 (b) *CLERICAL AMENDMENT.—The table of contents in*
11 *section 1(b) of such Act is amended by adding after the item*
12 *relating to section 228 (as added by section 104) the fol-*
13 *lowing new item:*

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

14 **SEC. 106. STREAMLINING OF DEPARTMENT CYBERSECU-**
15 **RITY ORGANIZATION.**

16 (a) *CYBERSECURITY AND INFRASTRUCTURE PROTEC-*
17 *TION DIRECTORATE.—The National Protection and Pro-*
18 *grams Directorate of the Department of Homeland Security*
19 *shall, after the date of the enactment of this Act, be known*
20 *and designated as the “Cybersecurity and Infrastructure*
21 *Protection Directorate”. Any reference to the National Pro-*
22 *tection and Programs Directorate of the Department in any*
23 *law, regulation, map, document, record, or other paper of*
24 *the United States shall be deemed to be a reference to the*

1 *Cybersecurity and Infrastructure Protection Directorate of*
2 *the Department.*

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

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

9 “(K) *Under Secretary for Cybersecurity and*
10 *Infrastructure Protection.*”

11 “(L) *Deputy Under Secretary for Cyberse-*
12 *curity.*”

13 “(M) *Deputy Under Secretary for Infra-*
14 *structure Protection.*”.

15 (2) *CONTINUATION IN OFFICE.—The individuals*
16 *who hold the positions referred to in subparagraphs*
17 *(K), (L), and (M) of subsection (a) of section 103 of*
18 *the Homeland Security Act of 2002 (as added by*
19 *paragraph (1) of this subsection) as of the date of the*
20 *enactment of this Act may continue to hold such posi-*
21 *tions.*

22 (c) *REPORT ON IMPROVING THE CAPABILITY AND EF-*
23 *ECTIVENESS OF THE CYBERSECURITY AND COMMUNICA-*
24 *TIONS OFFICE.—To improve the operational capability and*
25 *effectiveness in carrying out the cybersecurity mission (as*

1 *such term is defined in section 2 of the Homeland Security*
2 *Act of 2002, as amended by section 101) of the Department*
3 *of Homeland Security, the Secretary of Homeland Security*
4 *shall submit to the Committee on Homeland Security of the*
5 *House of Representatives and the Committee on Homeland*
6 *Security and Governmental Affairs of the Senate a report*
7 *on—*

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

11 (2) *recommendations for restructuring the*
12 *SAFETY Act Office within the Department to protect*
13 *and maintain operations in accordance with the Of-*
14 *ice's mission to provide incentives for the develop-*
15 *ment and deployment of anti-terrorism technologies*
16 *while elevating the profile and mission of the Office,*
17 *including the feasibility of utilizing third-party reg-*
18 *istrars for improving the throughput and effectiveness*
19 *of the certification process.*

20 (d) *REPORT ON CYBERSECURITY ACQUISITION CAPA-*
21 *BILITIES.—The Secretary of Homeland Security shall as-*
22 *sess the effectiveness of the Department of Homeland Secu-*
23 *rity's acquisition processes and the use of existing authori-*
24 *ties for acquiring cybersecurity technologies to ensure that*
25 *such processes and authorities are capable of meeting the*

1 *needs and demands of the Department's cybersecurity mis-*
2 *sion (as such term is defined in section 2 of the Homeland*
3 *Security Act of 2002, as amended by section 101). Not later*
4 *than 180 days after the date of the enactment of this Act,*
5 *the Secretary shall submit to the Committee on Homeland*
6 *Security of the House of Representatives and the Committee*
7 *on Homeland Security and Governmental Affairs of the*
8 *Senate a report on the effectiveness of the Department's ac-*
9 *quisition processes for cybersecurity technologies.*

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

18 **TITLE II—PUBLIC-PRIVATE COL-**
19 **LABORATION ON CYBERSECU-**
20 **RITY**

21 **SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
22 **CURITY.**

23 *(a) NATIONAL INSTITUTE OF STANDARDS AND TECH-*
24 *NOLOGY.—*

1 (1) *IN GENERAL.*—*The Director of the National*
2 *Institute of Standards and Technology, in coordina-*
3 *tion with the Secretary of Homeland Security, shall,*
4 *on an ongoing basis, facilitate and support the devel-*
5 *opment of a voluntary, industry-led set of standards,*
6 *guidelines, best practices, methodologies, procedures,*
7 *and processes to reduce cyber risks to critical infra-*
8 *structure. The Director, in coordination with the Sec-*
9 *retary—*

10 (A) *shall—*

11 (i) *coordinate closely and continuously*
12 *with relevant private entities, critical infra-*
13 *structure owners and critical infrastructure*
14 *operators, Sector Coordinating Councils, In-*
15 *formation Sharing and Analysis Centers,*
16 *and other relevant industry organizations,*
17 *and incorporate industry expertise to the*
18 *fullest extent possible;*

19 (ii) *consult with the Sector Specific*
20 *Agencies, Federal, State and local govern-*
21 *ments, the governments of other countries,*
22 *and international organizations;*

23 (iii) *utilize a prioritized, flexible, re-*
24 *peatable, performance-based, and cost-effec-*
25 *tive approach, including information secu-*

1 *rity measures and controls, that may be vol-*
2 *untarily adopted by critical infrastructure*
3 *owners and critical infrastructure operators*
4 *to help them identify, assess, and manage*
5 *cyber risks;*

6 *(iv) include methodologies to—*

7 *(I) identify and mitigate impacts*
8 *of the cybersecurity measures or con-*
9 *trols on business confidentiality; and*

10 *(II) protect individual privacy*
11 *and civil liberties;*

12 *(v) incorporate voluntary consensus*
13 *standards and industry best practices, and*
14 *align with voluntary international stand-*
15 *ards to the fullest extent possible;*

16 *(vi) prevent duplication of existing*
17 *regulatory processes and prevent conflict*
18 *with or superseding of existing regulatory*
19 *requirements and processes; and*

20 *(vii) include such other similar and*
21 *consistent elements as determined necessary;*
22 *and*

23 *(B) shall not prescribe or otherwise re-*
24 *quire—*

25 *(i) the use of specific solutions;*

1 (ii) the use of specific information
2 technology products or services; or

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

6 (2) *LIMITATION.*—Information shared with or
7 provided to the Director of the National Institute of
8 Standards and Technology or the Secretary of Home-
9 land Security for the purpose of the activities under
10 paragraph (1) may not be used by any Federal,
11 State, or local government department or agency to
12 regulate the activity of any private entity.

13 (b) *AMENDMENT.*—

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

18 “**SEC. 230. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**
19 **CURITY.**

20 “(a) *MEETINGS.*—The Secretary shall meet with the
21 Sector Coordinating Council for each critical infrastructure
22 sector designated under section 227(b) on a biannual basis
23 to discuss the cybersecurity threat to critical infrastructure,
24 voluntary activities to address cybersecurity, and ideas to

1 *improve the public-private partnership to enhance cyberse-*
2 *curity, in which the Secretary shall—*

3 “(1) *provide each Sector Coordinating Council*
4 *an assessment of the cybersecurity threat to each crit-*
5 *ical infrastructure sector designated under section*
6 *227(b), including information relating to—*

7 “(A) *any actual or assessed cyber threat, in-*
8 *cluding a consideration of adversary capability*
9 *and intent, preparedness, target attractiveness,*
10 *and deterrence capabilities;*

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

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

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

1 “(2) *provide recommendations, which may be*
2 *voluntarily adopted, on ways to improve cybersecu-*
3 *rity of critical infrastructure.*

4 “(b) *REPORT.—*

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

20 “(A) *the risk to each critical infrastructure*
21 *sector, including known cyber threats,*
22 *vulnerabilities, and potential consequences;*

23 “(B) *the extent and nature of any cyberse-*
24 *curity incidents during the previous year, in-*
25 *cluding the extent to which cyber incidents jeop-*

1 *ardized or imminently jeopardized information*
2 *systems;*

3 “(C) *the current status of the voluntary, in-*
4 *dustry-led set of standards, guidelines, best prac-*
5 *tices, methodologies, procedures, and processes to*
6 *reduce cyber risks within each critical infra-*
7 *structure sector; and*

8 “(D) *the volume and range of voluntary*
9 *technical assistance sought and provided by the*
10 *Department to each critical infrastructure sector.*

11 “(2) *SECTOR COORDINATING COUNCIL RE-*
12 *SPONSE.—Before making public and submitting each*
13 *report required under paragraph (1), the Secretary*
14 *shall provide a draft of each report to the Sector Co-*
15 *ordinating Council for the critical infrastructure sec-*
16 *tor covered by each such report. The Sector Coordi-*
17 *nating Council at issue may provide to the Secretary*
18 *a written response to such report within 45 days of*
19 *receiving the draft. If such Sector Coordinating Coun-*
20 *cil provides a written response, the Secretary shall in-*
21 *clude such written response in the final version of*
22 *each report required under paragraph (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 ac-*

1 *tivities under subsections (a) and (b) may not be used by*
 2 *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. 441*
 11 *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-ter-*
 20 *rorism”;*

21 (C) *in paragraphs (3), (4), and (5), by in-*
 22 *serting “or cybersecurity” after “anti-terrorism”*
 23 *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 ap-
14 pears;

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-TERRORISM”;

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 Secretary
12 determines meets the requirements under sub-
13 paragraph (B), as such requirements are further
14 defined and specified by the Secretary.

15 “(B) *REQUIREMENTS.*—A qualifying cyber
16 incident meets the requirements of this subpara-
17 graph 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 and
25 data that are essential to their reliable oper-

1 *ation, electronic storage devices, or any*
2 *other information system, or the informa-*
3 *tion that system controls, processes, stores,*
4 *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, assets,*
17 *information, or intellectual property*
18 *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 appro-*
13 *priated for each of fiscal years 2014, 2015, and 2016 for*
14 *the Department of Homeland Security, the Secretary of*
15 *Homeland Security is authorized to use not less than*
16 *\$20,000,000 for any such year for the Department’s SAFE-*
17 *TY Act Office.*

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

19 *This Act and the amendments made by this Act (except*
20 *that this section shall not apply in the case of section 202*
21 *of this Act and the amendments made by such section 202)*
22 *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 existing regulatory re-*
3 *quirements, mandatory standards, or related proc-*
4 *esses.*

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

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

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 Secu-*
24 *rity's Centers of Excellence, as designated by the Secretary,*
25 *to enhance knowledge with respect to the unique challenges*

1 *of addressing cyber threats to critical infrastructure. Eligi-*
2 *ble candidates shall possess necessary security clearances*
3 *and have a history of working with Federal agencies in*
4 *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” or
17 the “SMART Study”. In conducting such research, the Na-
18 tional 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 identi-*
23 *fication of the scale and scope of any potential sig-*
24 *nificant health and environmental impacts;*

1 (2) consider the forces affecting the grid, includ-
2 ing technical, economic, regulatory, environmental,
3 and geopolitical factors, and how such forces are like-
4 ly 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 af-
16 fecting 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 the implications of increased reliance
22 on digital information and control of the power grid
23 for improving reliability, resilience, and congestion
24 and for potentially increasing vulnerability to cyber
25 attack;

1 (5) review regulatory, industry, and institu-
2 tional factors and programs affecting the future of the
3 grid;

4 (6) research the costs and benefits, as well as the
5 strengths and weaknesses, of the options identified
6 under paragraph (1) to address the emerging forces
7 described in paragraph (2) that are shaping the grid;

8 (7) identify the barriers to realizing the options
9 identified and suggest strategies for overcoming those
10 barriers including suggested actions, priorities, incen-
11 tives, and possible legislative and executive actions;
12 and

13 (8) research the ability of the grid to integrate
14 existing and future infrastructure, including utilities,
15 telecommunications lines, highways, and other crit-
16 ical infrastructure.

17 (b) COOPERATION AND ACCESS TO INFORMATION AND
18 PERSONNEL.—The Secretary shall ensure that the National
19 Research Council receives full and timely cooperation, in-
20 cluding full access to information and personnel, from the
21 Department of Homeland Security, the Department of En-
22 ergy, including the management and operating components
23 of the Departments, and other Federal departments and
24 agencies, as necessary, for the purposes of conducting the
25 study described in subsection (a).

1 (c) *REPORT.*—

2 (1) *IN GENERAL.*—Not later than 18 months
3 from the date on which the Secretary enters into the
4 agreement with the National Research Council de-
5 scribed in subsection (a), the National Research
6 Council shall submit to the Secretary and the Com-
7 mittee on Homeland Security of the House of Rep-
8 resentatives and the Committee on Homeland Secu-
9 rity and Governmental Affairs of the Senate a report
10 containing the findings of the research required by
11 that subsection.

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

15 (d) *FUNDING.*—Of the amounts authorized to be ap-
16 propriated for 2014 for the Department of Homeland Secu-
17 rity, the Secretary of Homeland Security is authorized to
18 obligate and expend not more than \$2,000,000 for the Na-
19 tional Research Council report.

20 **TITLE III—HOMELAND SECURITY**
21 **CYBERSECURITY WORKFORCE**

22 **SEC. 301. HOMELAND SECURITY CYBERSECURITY WORK-**
23 **FORCE.**

24 (a) *IN GENERAL.*—Subtitle C of title II of the Home-
25 land Security Act of 2002, as amended by sections 101, 102,

1 103, 104, 105, and 201, is further amended by adding at
2 the end the following new section:

3 **“SEC. 230A. CYBERSECURITY OCCUPATION CATEGORIES,**
4 **WORKFORCE ASSESSMENT, AND STRATEGY.**

5 “(a) *SHORT TITLE.*—*This section may be cited as the*
6 *‘Homeland Security Cybersecurity Boots-on-the-Ground*
7 *Act’.*

8 “(b) *CYBERSECURITY OCCUPATION CATEGORIES.*—

9 “(1) *IN GENERAL.*—*Not later than 90 days after*
10 *the date of the enactment of this section, the Secretary*
11 *shall develop and issue comprehensive occupation cat-*
12 *egories for individuals performing activities in fur-*
13 *therance of the cybersecurity mission of the Depart-*
14 *ment.*

15 “(2) *APPLICABILITY.*—*The Secretary shall ensure*
16 *that the comprehensive occupation categories issued*
17 *under paragraph (1) are used throughout the Depart-*
18 *ment and are made available to other Federal agen-*
19 *cies.*

20 “(c) *CYBERSECURITY WORKFORCE ASSESSMENT.*—

21 “(1) *IN GENERAL.*—*Not later than 180 days*
22 *after the date of the enactment of this section and an-*
23 *nually thereafter, the Secretary shall assess the readi-*
24 *ness and capacity of the workforce of the Department*
25 *to meet its cybersecurity mission.*

1 “(2) *CONTENTS.*—*The assessment required under*
2 *paragraph (1) shall, at a minimum, include the fol-*
3 *lowing:*

4 “(A) *Information where cybersecurity posi-*
5 *tions are located within the Department, speci-*
6 *fied in accordance with the cybersecurity occupa-*
7 *tion categories issued under subsection (b).*

8 “(B) *Information on which cybersecurity*
9 *positions are—*

10 “(i) *performed by—*

11 “(I) *permanent full time depart-*
12 *mental employees, together with demo-*
13 *graphic information about such em-*
14 *ployees’ race, ethnicity, gender, dis-*
15 *ability status, and veterans status;*

16 “(II) *individuals employed by*
17 *independent contractors; and*

18 “(III) *individuals employed by*
19 *other Federal agencies, including the*
20 *National Security Agency; and*

21 “(ii) *vacant.*

22 “(C) *The number of individuals hired by*
23 *the Department pursuant to the authority grant-*
24 *ed to the Secretary in 2009 to permit the Sec-*
25 *retary to fill 1,000 cybersecurity positions across*

1 *the Department over a three year period, and in-*
2 *formation on what challenges, if any, were en-*
3 *countered with respect to the implementation of*
4 *such authority.*

5 “(D) *Information on vacancies within the*
6 *Department’s cybersecurity supervisory work-*
7 *force, from first line supervisory positions*
8 *through senior departmental cybersecurity posi-*
9 *tions.*

10 “(E) *Information on the percentage of indi-*
11 *viduals within each cybersecurity occupation*
12 *category who received essential training to per-*
13 *form their jobs, and in cases in which such*
14 *training is not received, information on what*
15 *challenges, if any, were encountered with respect*
16 *to the provision of such training.*

17 “(F) *Information on recruiting costs in-*
18 *curring with respect to efforts to fill cybersecurity*
19 *positions across the Department in a manner*
20 *that allows for tracking of overall recruiting and*
21 *identifying areas for better coordination and*
22 *leveraging of resources within the Department.*

23 “(d) *WORKFORCE STRATEGY.—*

24 “(1) *IN GENERAL.—Not later than 180 days*
25 *after the date of the enactment of this section, the Sec-*

1 *retary shall develop, maintain, and, as necessary, up-*
2 *date, a comprehensive workforce strategy that en-*
3 *hances the readiness, capacity, training, recruitment,*
4 *and retention of the cybersecurity workforce of the De-*
5 *partment.*

6 *“(2) CONTENTS.—The comprehensive workforce*
7 *strategy developed under paragraph (1) shall in-*
8 *clude—*

9 *“(A) a multiphased recruitment plan, in-*
10 *cluding relating to experienced professionals,*
11 *members of disadvantaged or underserved com-*
12 *munities, the unemployed, and veterans;*

13 *“(B) a 5-year implementation plan;*

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

16 *“(D) obstacles impeding the hiring and de-*
17 *velopment of a cybersecurity workforce at the De-*
18 *partment.*

19 *“(e) INFORMATION SECURITY TRAINING.—Not later*
20 *than 270 days after the date of the enactment of this section,*
21 *the Secretary shall establish and maintain a process to*
22 *verify on an ongoing basis that individuals employed by*
23 *independent contractors who serve in cybersecurity posi-*
24 *tions at the Department receive initial and recurrent infor-*
25 *mation security training comprised of general security*

1 *awareness training necessary to perform their job functions,*
2 *and role-based security training that is commensurate with*
3 *assigned responsibilities. The Secretary shall maintain doc-*
4 *umentation to ensure that training provided to an indi-*
5 *vidual under this subsection meets or exceeds requirements*
6 *for such individual's job function.*

7 “(f) *UPDATES.*—*The Secretary shall submit to the ap-*
8 *propriate congressional committees annual updates regard-*
9 *ing the cybersecurity workforce assessment required under*
10 *subsection (c), information on the progress of carrying out*
11 *the comprehensive workforce strategy developed under sub-*
12 *section (d), and information on the status of the implemen-*
13 *tation of the information security training required under*
14 *subsection (e).*

15 “(g) *GAO STUDY.*—*The Secretary shall provide the*
16 *Comptroller General of the United States with information*
17 *on the cybersecurity workforce assessment required under*
18 *subsection (c) and progress on carrying out the comprehen-*
19 *sive workforce strategy developed under subsection (d). The*
20 *Comptroller General shall submit to the Secretary and the*
21 *appropriate congressional committees a study on such as-*
22 *essment and strategy.*

23 “(h) *CYBERSECURITY FELLOWSHIP PROGRAM.*—*Not*
24 *later than 120 days after the date of the enactment of this*
25 *section, the Secretary shall submit to the appropriate con-*

1 *gressional committees a report on the feasibility of estab-*
 2 *lishing a Cybersecurity Fellowship Program to offer a tui-*
 3 *tion payment plan for undergraduate and doctoral can-*
 4 *didates who agree to work for the Department for an agreed-*
 5 *upon period of time.”.*

6 (b) *CLERICAL AMENDMENT.*—*The table of contents in*
 7 *section 1(b) of such Act is amended by adding after the item*
 8 *relating to section 230 (as added by section 201) the fol-*
 9 *lowing new item:*

“Sec. 230A. Cybersecurity occupation categories, workforce assessment, and strat-
egy.”.

10 **SEC. 302. PERSONNEL AUTHORITIES.**

11 (a) *IN GENERAL.*—*Subtitle C of title II of the Home-*
 12 *land Security Act of 2002, as amended by sections 101, 102,*
 13 *103, 104, 105, 106, 201, and 301 is further amended by*
 14 *adding at the end the following new section:*

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

16 *“(a) IN GENERAL.—*

17 *“(1) PERSONNEL AUTHORITIES.—The Secretary*
 18 *may exercise with respect to qualified employees of the*
 19 *Department the same authority that the Secretary of*
 20 *Defense has with respect to civilian intelligence per-*
 21 *sonnel and the scholarship program under sections*
 22 *1601, 1602, 1603, and 2200a of title 10, United*
 23 *States Code, to establish as positions in the excepted*
 24 *service, appoint individuals to such positions, fix*

1 *pay, and pay a retention bonus to any employee ap-*
2 *pointed under this section if the Secretary determines*
3 *that such is needed to retain essential personnel. Be-*
4 *fore announcing the payment of a bonus under this*
5 *paragraph, the Secretary shall submit to the Com-*
6 *mittee on Homeland Security of the House of Rep-*
7 *resentatives and the Committee on Homeland Secu-*
8 *rity and Governmental Affairs of the Senate a writ-*
9 *ten explanation of such determination. Such author-*
10 *ity shall be exercised—*

11 *“(A) to the same extent and subject to the*
12 *same conditions and limitations that the Sec-*
13 *retary of Defense may exercise such authority*
14 *with respect to civilian intelligence personnel of*
15 *the Department of Defense; and*

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

19 *“(2) CIVIL SERVICE PROTECTIONS.—Sections*
20 *1221 and 2302, and chapter 75 of title 5, United*
21 *States Code, shall apply to the positions established*
22 *pursuant to the authorities provided under paragraph*
23 *(1).*

24 *“(3) PLAN FOR EXECUTION OF AUTHORITIES.—*
25 *Not later than 120 days after the date of the enact-*

1 *ment of this section, the Secretary shall submit to the*
2 *Committee on Homeland Security of the House of*
3 *Representatives and the Committee on Homeland Se-*
4 *curity and Governmental Affairs of the Senate a re-*
5 *port that contains a plan for the use of the authorities*
6 *provided under this subsection.*

7 *“(b) ANNUAL REPORT.—Not later than one year after*
8 *the date of the enactment of this section and annually there-*
9 *after for four years, the Secretary shall submit to the Com-*
10 *mittee on Homeland Security of the House of Representa-*
11 *tives and the Committee on Homeland Security and Gov-*
12 *ernmental Affairs of the Senate a detailed report (including*
13 *appropriate metrics on actions occurring during the report-*
14 *ing period) that discusses the processes used by the Sec-*
15 *retary in implementing this section and accepting applica-*
16 *tions, assessing candidates, ensuring adherence to veterans’*
17 *preference, and selecting applicants for vacancies to be filled*
18 *by a qualified employee.*

19 *“(c) DEFINITION OF QUALIFIED EMPLOYEE.—In this*
20 *section, the term ‘qualified employee’ means an employee*
21 *who performs functions relating to the security of Federal*
22 *civilian information systems, critical infrastructure infor-*
23 *mation systems, or networks of either of such systems.”.*

24 *(b) CLERICAL AMENDMENT.—The table of contents in*
25 *section 1(b) of such Act is amended by adding after the item*

- 1 *relating to section 230A (as added by section 301) the fol-*
- 2 *lowing new item:*

“Sec. 230B. Personnel authorities.”.

Union Calendar No. 411

113TH CONGRESS
2^D SESSION

H. R. 3696

[Report No. 113-550, Part I]

A BILL

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

JULY 23, 2014

Reported from the Committee on Homeland Security
with an amendment

JULY 23, 2014

The Committees on Science, Space, and Technology and Oversight and Government Reform discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed