

113TH CONGRESS  
1ST SESSION

# H. R. 3696

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

---

## 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 2013”.

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. Assessment of cybersecurity workforce.  
 Sec. 107. Personnel authorities.  
 Sec. 108. 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.

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

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

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

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

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

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

1           “(22) The term ‘cyber incident’ means an inci-  
2           dent resulting in, or an attempt to cause an incident  
3           that, if successful, would—

4                   “(A) jeopardize or imminently jeopardize,  
5                   without lawful authority, the security, integrity,  
6                   confidentiality, or availability of an information  
7                   system or network of information systems or  
8                   any information stored on, processed on, or  
9                   transiting such a system;

10                   “(B) constitute a violation or imminent  
11                   threat of violation of law, security policies, secu-  
12                   rity procedures, or acceptable use policies re-  
13                   lated to an information system or network of  
14                   information systems, or an act of terrorism  
15                   against an information system or network of in-  
16                   formation systems; or

17                   “(C) result in the denial of access to or  
18                   degradation, disruption, or destruction of an in-  
19                   formation system or network of information  
20                   systems, or the defeat of an operations control  
21                   or technical control essential to the security or  
22                   operation of an information system or network  
23                   of information systems.

1           “(23) The term ‘cybersecurity provider’ means  
2 a non-Federal entity that provides goods or services  
3 intended to be used for cybersecurity purposes.

4           “(24) The term ‘cybersecurity purpose’ means  
5 the purpose of ensuring the security, integrity, con-  
6 fidentiality, or availability of, or safeguarding, an in-  
7 formation system or network of information systems,  
8 including protecting an information system or net-  
9 work of information systems, or data residing on an  
10 information system or network of information sys-  
11 tems, including protection of an information system  
12 or network of information systems, from—

13                   “(A) a vulnerability of an information sys-  
14 tem or network of information systems;

15                   “(B) a threat to 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                   “(C) efforts to deny access to or degrade,  
21 disrupt, or destroy an information system or  
22 network of information systems; or

23                   “(D) efforts to gain unauthorized access to  
24 an information system or network of informa-  
25 tion systems, including to gain such unauthor-

1           ized access for the purpose of exfiltrating infor-  
2           mation stored on, processed on, or transiting  
3           such a system or network.

4           “(25) The term ‘cybersecurity system’ means a  
5           system designed or employed to ensure the security,  
6           integrity, confidentiality, or availability of, or safe-  
7           guard, an information system or network of informa-  
8           tion systems, including protecting such a system or  
9           network from—

10                   “(A) a vulnerability of an information sys-  
11                   tem or network of information systems;

12                   “(B) a threat to the security, integrity,  
13                   confidentiality, or availability of an information  
14                   system or network of information systems or  
15                   any information stored on, processed on, or  
16                   transiting such a system or network;

17                   “(C) efforts to deny access to or degrade,  
18                   disrupt, or destroy an information system or  
19                   network of information systems of a private en-  
20                   tity; or

21                   “(D) efforts to gain unauthorized access to  
22                   an information system or network of informa-  
23                   tion systems, including to gain such unauthor-  
24                   ized access for the purpose of exfiltrating infor-

1           mation stored on, processed on, or transiting  
2           such a system or network.

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

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

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

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

22                 “(C) efforts to deny access to or degrade,  
23                 disrupt, or destroy an information system or  
24                 network of information systems of a govern-  
25                 ment or private entity;

1           “(D) efforts to gain unauthorized access to  
2           an information system or network of informa-  
3           tion systems of a government or private entity,  
4           including to gain such unauthorized access for  
5           the purpose of exfiltrating information stored  
6           on, processed on, or transiting such a system or  
7           network; or

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

11          “(28) The term ‘Federal civilian information  
12          systems’—

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

20                 “(B) does not include—

21                         “(i) a national security system; or

22                         “(ii) information, information sys-  
23                         tems, and networks of information systems  
24                         that are owned, operated, controlled, or li-  
25                         censed solely for use by, or on behalf of,

1           the Department of Defense, a military de-  
2           partment, or an element of the intelligence  
3           community.

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

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

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

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

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

1           “(31) The term ‘private entity’ means any indi-  
2           vidual or any private or publically-traded company,  
3           public or private utility, organization, or corporation,  
4           including an officer, employee, or agent thereof.

5           “(32) The term ‘protected private entity’ means  
6           an entity, other than an individual, that enters into  
7           a contract with a cybersecurity provider for goods  
8           and services to be used for cybersecurity purposes.

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

14 **SEC. 102. ENHANCEMENT OF CYBERSECURITY.**

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

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

19          “The Secretary, in collaboration with the heads of  
20          other appropriate Federal Government entities, shall con-  
21          duct activities for cybersecurity purposes, including the  
22          provision of shared situational awareness to each other to  
23          enable real-time, integrated, and operational actions to  
24          protect from, prevent, mitigate, respond to, and recover  
25          from cyber incidents.”.

1 (b) CLERICAL AMENDMENTS.—

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

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

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

9 (A) by adding after the item relating to  
10 section 225 the following new item:

“Sec. 226. Enhancement of cybersecurity.”;

11 and

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

“Subtitle C—Cybersecurity and Information Sharing”.

15 **SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE**  
16 **AND INFORMATION SHARING.**

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

21 **“SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE**  
22 **AND INFORMATION SHARING.**

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

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

6                   “(A) facilitate a national effort to  
7                   strengthen and maintain secure, functioning,  
8                   and resilient critical infrastructure from cyber  
9                   threats;

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

15                   “(C) seek industry sector-specific expertise  
16                   to—

17                           “(i) assist in the development of vol-  
18                           untary security and resiliency strategies;  
19                           and

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

24                   “(D) upon request, facilitate and assist  
25                   risk management efforts of entities to reduce

1 vulnerabilities, identify and disrupt threats, and  
2 minimize consequences to their critical infra-  
3 structure;

4 “(E) upon request, provide education and  
5 assistance to critical infrastructure owners and  
6 critical infrastructure operators on how they  
7 may use protective measures and counter-  
8 measures to strengthen the security and resil-  
9 ience of the Nation’s critical infrastructure; and

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

14 “(2) ADDITIONAL RESPONSIBILITIES.—The  
15 Secretary shall—

16 “(A) manage Federal efforts to secure,  
17 protect, and ensure the resiliency of Federal ci-  
18 vilian information systems, and, upon request,  
19 support critical infrastructure owners’ and crit-  
20 ical infrastructure operators’ efforts to secure,  
21 protect, and ensure the resiliency of critical in-  
22 frastructure from cyber threats;

23 “(B) direct an entity within the Depart-  
24 ment to serve as a Federal civilian entity by  
25 and among Federal, State, and local govern-

1           ments, private entities, and critical infrastruc-  
2           ture sectors to provide multi-directional sharing  
3           of real-time, actionable, and relevant cyber  
4           threat information;

5           “(C) promote a national awareness effort  
6           to educate the general public on the importance  
7           of securing information systems;

8           “(D) upon request, facilitate expeditious  
9           cyber incident response and recovery assistance,  
10          and provide analysis and warnings related to  
11          threats to and vulnerabilities of critical infor-  
12          mation systems, crisis and consequence man-  
13          agement support, and other remote or on-site  
14          technical assistance with the heads of other ap-  
15          propriate Federal agencies to Federal, State,  
16          and local government entities and private enti-  
17          ties for cyber incidents affecting critical infra-  
18          structure; and

19          “(E) engage with international partners to  
20          strengthen the security and resilience of domes-  
21          tic critical infrastructure and critical infrastruc-  
22          ture located outside of the United States upon  
23          which the United States depends.

24          “(3) RULE OF CONSTRUCTION.—Nothing in  
25          this section may be construed to require any private

1       entity to request assistance from the Secretary, or  
2       require any private entity requesting such assistance  
3       to implement any measure or recommendation sug-  
4       gested by the Secretary.

5       “(b) CRITICAL INFRASTRUCTURE SECTORS.—The  
6       Secretary, in collaboration with the heads of other appro-  
7       priate Federal agencies, shall designate critical infrastruc-  
8       ture sectors (that may include subdivisions of sectors with-  
9       in a sector as the Secretary may determine appropriate).  
10      The critical infrastructure sectors designated under this  
11      subsection may include the following:

12             “(1) Chemical.

13             “(2) Commercial facilities.

14             “(3) Communications.

15             “(4) Critical manufacturing.

16             “(5) Dams.

17             “(6) Defense Industrial Base.

18             “(7) Emergency services.

19             “(8) Energy.

20             “(9) Financial services.

21             “(10) Food and agriculture.

22             “(11) Government facilities.

23             “(12) Healthcare and public health.

24             “(13) Information technology.

25             “(14) Nuclear reactors, materials, and waste.

1           “(15) Transportation systems.

2           “(16) Water and wastewater systems.

3           “(17) Such other sectors as the Secretary de-  
4           termines appropriate.

5           “(c) SECTOR SPECIFIC AGENCIES.—The Secretary,  
6 in collaboration with the relevant critical infrastructure  
7 sector and the heads of other appropriate Federal agen-  
8 cies, shall recognize the Federal agency designated as of  
9 November 1, 2013, as the ‘Sector Specific Agency’ for  
10 each critical infrastructure sector designated under sub-  
11 section (b). If the designated Sector Specific Agency for  
12 a particular critical infrastructure sector is the Depart-  
13 ment, for the purposes of this section, the Secretary shall  
14 carry out this section. The Secretary, in coordination with  
15 the heads of each such Sector Specific Agency shall—

16           “(1) support the security and resilience activi-  
17           ties of the relevant critical infrastructure sector in  
18           accordance with this subtitle; and

19           “(2) provide institutional knowledge and spe-  
20           cialized expertise to the relevant critical infrastruc-  
21           ture sector.

22           “(d) SECTOR COORDINATING COUNCILS.—

23           “(1) RECOGNITION.—The Secretary, in collabo-  
24           ration with each critical infrastructure sector and  
25           the relevant Sector Specific Agency, shall recognize

1 the Sector Coordinating Council for each critical in-  
2 frastructure sector designated under subsection (b)  
3 to coordinate with each such sector on security and  
4 resilience activities and emergency response and re-  
5 covery efforts.

6 “(2) MEMBERSHIP.—

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

10 “(i) be comprised exclusively of rel-  
11 evant critical infrastructure owners, critical  
12 infrastructure operators, private entities,  
13 and representative trade associations for  
14 the sector;

15 “(ii) reflect the unique composition of  
16 each sector; and

17 “(iii) include relevant small, medium,  
18 and large critical infrastructure owners,  
19 critical infrastructure operators, private  
20 entities, and representative trade associa-  
21 tions for the sector.

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

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

4                   “(A) serve as a self-governing, self-orga-  
5                   nized primary policy, planning, and strategic  
6                   communications entity for coordinating with the  
7                   Department, the relevant Sector-Specific Agen-  
8                   cy designated under subsection (c), and the rel-  
9                   evant Information Sharing and Analysis Cen-  
10                  ters under subsection (e) on security and resil-  
11                  ience activities and emergency response and re-  
12                  covery efforts;

13                  “(B) establish governance and operating  
14                  procedures, and designate a chairperson for the  
15                  sector to carry out the activities described in  
16                  this subsection;

17                  “(C) coordinate with the Department, the  
18                  relevant Information Sharing and Analysis Cen-  
19                  ters under subsection (e), and other Sector Co-  
20                  ordinating Councils to update, maintain, and  
21                  exercise the National Cybersecurity Incident  
22                  Response Plan in accordance with section  
23                  229(b); and

24                  “(D) provide any recommendations to the  
25                  Department on infrastructure protection tech-

1           nology gaps to help inform research and devel-  
2           opment efforts at the Department.

3           “(e) SECTOR INFORMATION SHARING AND ANALYSIS  
4 CENTERS.—

5           “(1) RECOGNITION.—The Secretary, in collabo-  
6           ration with the relevant Sector Coordinating Council  
7           and the critical infrastructure sector represented by  
8           such Council, and in coordination with the relevant  
9           Sector Specific Agency, shall recognize at least one  
10          Information Sharing and Analysis Center for each  
11          critical infrastructure sector designated under sub-  
12          section (b) for purposes of paragraph (3). No other  
13          Information Sharing and Analysis Organizations, in-  
14          cluding Information Sharing and Analysis Centers,  
15          may be precluded from having an information shar-  
16          ing relationship within the National Cybersecurity  
17          and Communications Integration Center established  
18          pursuant to section 228. Nothing in this subsection  
19          or any other provision of this subtitle may be con-  
20          strued to limit, restrict, or condition any private en-  
21          tity or activity utilized by, among, or between pri-  
22          vate entities.

23          “(2) ROLES AND RESPONSIBILITIES.—In addi-  
24          tion to such other activities as may be authorized by

1 law, at least one Information Sharing and Analysis  
2 Center for a critical infrastructure sector shall—

3 “(A) serve as an information sharing re-  
4 source for such sector and promote ongoing  
5 multi-directional sharing of real-time, relevant,  
6 and actionable cyber threat information and  
7 analysis by and among such sector, the Depart-  
8 ment, the relevant Sector Specific Agency, and  
9 other critical infrastructure sector Information  
10 Sharing and Analysis Centers;

11 “(B) establish governance and operating  
12 procedures to carry out the activities conducted  
13 under this subsection;

14 “(C) serve as an emergency response and  
15 recovery operations coordination point for such  
16 sector, and upon request, facilitate cyber inci-  
17 dent response capabilities in coordination with  
18 the Department, the relevant Sector Specific  
19 Agency and the relevant Sector Coordinating  
20 Council;

21 “(D) facilitate cross-sector coordination  
22 and sharing of cyber threat information to pre-  
23 vent related or consequential impacts to other  
24 critical infrastructure sectors;

1           “(E) coordinate with the Department, the  
2 relevant Sector Coordinating Council, the rel-  
3 evant Sector Specific Agency, and other critical  
4 infrastructure sector Information Sharing and  
5 Analysis Centers on the development, integra-  
6 tion, and implementation of procedures to sup-  
7 port technology neutral, real-time information  
8 sharing capabilities and mechanisms within the  
9 National Cybersecurity and Communications  
10 Integration Center established pursuant to sec-  
11 tion 228, including—

12                   “(i) the establishment of a mechanism  
13 to voluntarily report identified vulnerabili-  
14 ties and opportunities for improvement;

15                   “(ii) the establishment of metrics to  
16 assess the effectiveness and timeliness of  
17 the Department’s and Information Sharing  
18 and Analysis Centers’ information sharing  
19 capabilities; and

20                   “(iii) the establishment of a mecha-  
21 nism for anonymous suggestions and com-  
22 ments;

23           “(F) implement an integration and anal-  
24 ysis function to inform sector planning, risk  
25 mitigation, and operational activities regarding

1 the protection of each critical infrastructure  
2 sector from cyber incidents;

3 “(G) combine consequence, vulnerability,  
4 and threat information to share actionable as-  
5 sessments of critical infrastructure sector risks  
6 from cyber incidents;

7 “(H) coordinate with the Department, the  
8 relevant Sector Specific Agency, and the rel-  
9 evant Sector Coordinating Council to update,  
10 maintain, and exercise the National Cybersecu-  
11 rity Incident Response Plan in accordance with  
12 section 229(b); and

13 “(I) safeguard cyber threat information  
14 from unauthorized disclosure.

15 “(3) FUNDING.—Of the amounts authorized to  
16 be appropriated for each of fiscal years 2014, 2015,  
17 and 2016 for the Cybersecurity and Communications  
18 Office of the Department, the Secretary is author-  
19 ized to use not less than \$25,000,000 for any such  
20 year for operations support at the National Cyberse-  
21 curity and Communications Integration Center es-  
22 tablished under section 228(a) of all recognized In-  
23 formation Sharing and Analysis Centers under para-  
24 graph (1) of this subsection.

1           “(f) CLEARANCES.—The Secretary shall expedite the  
2 processing of security clearances under Executive Order  
3 13549 or successor orders to appropriate members of the  
4 Sector Coordinating Councils and the critical infrastruc-  
5 ture sector Information Sharing and Analysis Centers.

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

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

21                   “(2) develop procedures to ensure continuous,  
22 collaborative, and effective interactions between the  
23 Department, critical infrastructure owners, and crit-  
24 ical infrastructure operators; and

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

4           “(h) PROTECTION OF FEDERAL CIVILIAN INFORMA-  
5           TION SYSTEMS.—

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

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

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

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

22                   “(C) establish and sustain continuous  
23                   diagnostics systems for Federal civilian infor-  
24                   mation systems to aggregate data and identify

1 and prioritize the mitigation of cyber vulnerabil-  
2 ities in such systems for cybersecurity purposes;

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

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

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

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

23 “(H) develop minimum technology neutral  
24 operational requirements for network and secu-

1 rity operations centers to facilitate the protec-  
2 tion of all Federal civilian information systems;

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

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

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

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

24 “(3) USE OF CERTAIN COMMUNICATIONS.—

1           “(A) IN GENERAL.—The Secretary may  
2 enter into contracts or other agreements, or  
3 otherwise request and obtain, in accordance  
4 with applicable law, the assistance of private  
5 entities that provide electronic communication  
6 services, remote computing services, or cyberse-  
7 curity services to acquire, intercept, retain, use,  
8 and disclose communications and other system  
9 traffic, deploy countermeasures, or otherwise  
10 operate protective capabilities in accordance  
11 with subparagraphs (C), (D), (E), and (F) of  
12 paragraph (2). No cause of action shall exist  
13 against private entities for assistance provided  
14 to the Secretary in accordance with this sub-  
15 section.

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

18                   “(i) require or compel any private en-  
19 tity to enter in a contract or agreement de-  
20 scribed in such subparagraph; or

21                   “(ii) authorize the Secretary to take  
22 any action with respect to any communica-  
23 tions or system traffic transiting or resid-  
24 ing on any information system or network

1 of information systems other than a Fed-  
2 eral civilian information system.

3 “(i) **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  
8 in section 1(b) of such Act is amended by adding at the  
9 end of the items relating to such subtitle the following new  
10 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  
15 and 103, is further amended by adding at the end the  
16 following new section:

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

19 “(a) **ESTABLISHMENT.**—There is established in the  
20 Department the National Cybersecurity and Communica-  
21 tions Integration Center (referred to in this section as the  
22 ‘Center’), which shall be a Federal civilian information  
23 sharing interface that provides shared situational aware-  
24 ness to enable real-time, integrated, and operational ac-  
25 tions across the Federal Government, and share cyber

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

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

8 “(1) At least one Information Sharing and  
9 Analysis Center established under section 227(e) for  
10 each 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  
19 system owners and operators, and disseminate time-  
20 ly notifications regarding current and potential cyber  
21 threats and vulnerabilities.

22 “(4) The Industrial Control System Cyber  
23 Emergency Response Team to coordinate with in-  
24 dustrial control systems owners and operators and

1 share industrial control systems-related security inci-  
2 dents and mitigation measures.

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

7 “(6) Such other Federal, State, and local gov-  
8 ernment entities, private entities, organizations, or  
9 individuals as the Secretary may consider appro-  
10 priate 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  
14 as 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 en-  
7           tities that own or operate information systems or  
8           networks of information systems to protect from,  
9           prevent, mitigate, respond to, and recover from  
10          cyber incidents;

11          “(4) facilitate cross-sector coordination and  
12          sharing of cyber threat information to prevent re-  
13          lated or consequential impacts to other critical infra-  
14          structure sectors;

15          “(5) collaborate with the Sector Coordinating  
16          Councils, Information Sharing and Analysis Centers,  
17          Sector Specific Agencies, and the relevant critical in-  
18          frastructure sectors on the development and imple-  
19          mentation of procedures to support technology neu-  
20          tral real-time information sharing capabilities and  
21          mechanisms;

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 to identify requirements for data

1 and information formats and accessibility, system  
2 interoperability, and redundant systems and alter-  
3 native capabilities in the event of a disruption in the  
4 primary information sharing capabilities and mecha-  
5 nisms at the Center;

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

9 “(8) safeguard sensitive cyber threat informa-  
10 tion from unauthorized disclosure;

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

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

21 “(B) provide to the Center cyber incident  
22 detection, analysis, mitigation, and response in-  
23 formation; and

1           “(C) immediately send and disclose to the  
2           Center cyber threat information received by  
3           such agencies; and

4           “(10) perform such other duties as the Sec-  
5           retary may require to facilitate a national effort to  
6           strengthen and maintain secure, functioning, and re-  
7           silient critical infrastructure from cyber threats.

8           “(e) INTEGRATION AND ANALYSIS.—The Center  
9           shall maintain an integration and analysis function, which  
10          shall —

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

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

1        iency of the critical infrastructure of the United  
2        States;

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

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

11        “(f) REPORT OF CYBER ATTACKS AGAINST FEDERAL  
12       GOVERNMENT NETWORKS.—The Secretary shall submit  
13       to the Committee on Homeland Security of the House of  
14       Representatives, the Committee on Homeland Security  
15       and Governmental Affairs of the Senate, and the Comp-  
16       troller General of the United States an annual report that  
17       summarizes major cyber incidents involving Federal civil-  
18       ian agency information systems and provides aggregate  
19       statistics on the number of breaches, the volume of data  
20       exfiltrated, the consequential impact, and the estimated  
21       cost of remedying such breaches.

22        “(g) REPORT ON THE OPERATIONS OF THE CEN-  
23       TER.—The Secretary, in consultation with the Sector Co-  
24       ordinating Councils and appropriate Federal Government  
25       entities, shall submit to the Committee on Homeland Se-

1 curity of the House of Representatives, the Committee on  
2 Homeland Security and Governmental Affairs of the Sen-  
3 ate, and the Comptroller General of the United States an  
4 annual report on—

5           “(1) the capability and capacity of the Center  
6           to carry out its cybersecurity mission in accordance  
7           with this section, and sections 226, 227, 229, 230,  
8           230A, and 230B;

9           “(2) the extent to which the Department is en-  
10          gaged in information sharing with each critical in-  
11          frastructure sector designated under section 227(b),  
12          including—

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

15                   “(B) the extent to which critical infra-  
16                   structure owners and critical infrastructure op-  
17                   erators of each critical infrastructure sector  
18                   participate in information sharing at the Cen-  
19                   ter;

20           “(3) the volume and range of activities with re-  
21          spect to which the Secretary collaborated with the  
22          Sector Coordinating Councils and the Sector-Specific  
23          Agencies to promote greater engagement with the  
24          Center; and



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

3 **“SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL**  
4 **ASSISTANCE.**

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

7 “(1) upon request, provide timely technical as-  
8 sistance and crisis management support to Federal,  
9 State, and local government entities, private entities,  
10 and critical infrastructure owners and critical infra-  
11 structure operators involving cyber incidents affect-  
12 ing critical infrastructure; and

13 “(2) upon request, provide actionable rec-  
14 ommendations on security and resilience measures  
15 and countermeasures to Federal, State, and local  
16 government entities, private entities, and critical in-  
17 frastructure owners and critical infrastructure oper-  
18 ators prior to, during, and after cyber incidents.

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

22 “(c) CYBER INCIDENT RESPONSE PLAN.—The Sec-  
23 retary, in coordination with the Sector Coordinating Coun-  
24 cils, Information Sharing and Analysis Centers, and Fed-  
25 eral, State, and local governments, shall develop, regularly

1 update, maintain, and exercise a National Cybersecurity  
2 Incident Response Plan which shall—

3 “(1) include effective emergency response plans  
4 associated with cyber threats to critical infrastruc-  
5 ture, information systems, or networks of informa-  
6 tion systems; and

7 “(2) ensure that such National Cybersecurity  
8 Incident Response Plan can adapt to and reflect a  
9 changing cyber threat environment, and incorporate  
10 best practices and lessons learned from regular exer-  
11 cises, training, and after-action reports.”.

12 (b) CLERICAL AMENDMENT.—The table of contents  
13 in section 1(b) of such Act, as amended by sections 103  
14 and 104, is further amended by adding at the end the  
15 following new item:

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

16 **SEC. 106. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

17 (a) IN GENERAL.—Subtitle C of title II of the Home-  
18 land Security Act of 2002, as amended by sections 101,  
19 103, 104, and 105, is further amended by adding at the  
20 end the following new section:

21 **“SEC. 230. ASSESSMENT OF CYBERSECURITY WORKFORCE.**

22 “(a) ASSESSMENT.—The Secretary, in consultation  
23 with relevant private entities, shall regularly assess the  
24 readiness and capacity of the workforce of the Department

1 to meet the needs of the cybersecurity mission of the De-  
2 partment.

3 “(b) STRATEGY REQUIRED.—Not later than 180  
4 days after the date of the enactment of this section, the  
5 Secretary shall develop, maintain, and, as necessary, up-  
6 date, a comprehensive workforce strategy designed to en-  
7 hance the readiness, capacity, training, recruitment, and  
8 retention of the cybersecurity personnel of the Depart-  
9 ment. Such strategy shall include a five-year plan on re-  
10 cruitment of personnel for the workforce of the Depart-  
11 ment, and ten-year projections of the workforce needs of  
12 the Department. The Secretary shall submit such strategy  
13 to the Committee on Homeland Security of the House of  
14 Representatives and the Committee on Homeland Security  
15 and Governmental Affairs of the Senate.”.

16 (b) CLERICAL AMENDMENT.—The table of contents  
17 in section 1(b) of such Act, as amended by sections 103,  
18 104, and 105, is further amended by adding at the end  
19 the following new item:

“230. Assessment of cybersecurity workforce.”.

20 **SEC. 107. PERSONNEL AUTHORITIES.**

21 (a) IN GENERAL.—Subtitle C of title II of the Home-  
22 land Security Act of 2002, as amended by sections 101,  
23 102, 103, 104, 105, and 106, is further amended by add-  
24 ing at the end the following new section:

1 **“SEC. 230A. PERSONNEL AUTHORITIES.**

2 “(a) IN GENERAL.—

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

21 “(A) to the same extent and subject to the  
22 same conditions and limitations that the Sec-  
23 retary of Defense may exercise such authority  
24 with respect to civilian intelligence personnel of  
25 the Department of Defense; and

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

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

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

17          “(b) ANNUAL REPORT.—Not later than one year  
18          after the date of the enactment of this section and annu-  
19          ally thereafter for four years, the Secretary shall submit  
20          to the Committee on Homeland Security of the House of  
21          Representatives and the Committee on Homeland Security  
22          and Governmental Affairs of the Senate a detailed report  
23          (including appropriate metrics on actions occurring during  
24          the reporting period) that discusses the processes used by  
25          the Secretary in implementing this section and accepting

1 applications, assessing candidates, ensuring adherence to  
2 veterans' preference, and selecting applicants for vacancies  
3 to be filled by a qualified employee.

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

10 (b) CLERICAL AMENDMENT.—The table of contents  
11 in section 1(b) of such Act, as amended by sections 103,  
12 104, 105, and 106, is further amended by adding at the  
13 end the following new item:

“230A. Personnel authorities.”.

14 **SEC. 108. STREAMLINING OF DEPARTMENT CYBERSECURI-**  
15 **TY ORGANIZATION.**

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

1 be a reference to the Cybersecurity and Infrastructure  
2 Protection Directorate of the Department.

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

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

9 “(K) Under Secretary for Cybersecurity  
10 and 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 individ-  
16 uals who hold the positions referred to in subpara-  
17 graphs (K), (L), and (M) of subsection (a) of section  
18 103 of the Homeland Security Act of 2002 (as  
19 added by paragraph (1) of this subsection) as of the  
20 date of the enactment of this Act may continue to  
21 hold such positions.

22 (c) REPORT ON IMPROVING THE CAPABILITY AND  
23 EFFECTIVENESS OF THE CYBERSECURITY AND COMMU-  
24 NICATIONS OFFICE.—To improve the operational capa-  
25 bility and effectiveness in carrying out the cybersecurity

1 mission of the Department of Homeland Security, the Sec-  
2 retary of Homeland Security shall submit to the Com-  
3 mittee on Homeland Security of the House of Representa-  
4 tives and the Committee on Homeland Security and Gov-  
5 ernmental Affairs of the Senate a report on—

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

9 (2) recommendations for restructuring the  
10 SAFETY Act Office within the Department to ele-  
11 vate the profile and mission of the Office, including  
12 the feasibility of utilizing third-party registrars for  
13 improving the throughput and effectiveness of the  
14 certification process.

15 (d) REPORT ON CYBERSECURITY ACQUISITION CAPA-  
16 BILITIES.—The Secretary of Homeland Security shall as-  
17 sess the effectiveness of the Department of Homeland Se-  
18 curity’s acquisition processes and the use of existing au-  
19 thorities for acquiring cybersecurity technologies to ensure  
20 that such processes and authorities are capable of meeting  
21 the needs and demands of the Department’s cybersecurity  
22 mission. Not later than 180 days after the date of the  
23 enactment of this Act, the Secretary shall submit to the  
24 Committee on Homeland Security of the House of Rep-  
25 resentatives and the Committee on Homeland Security

1 and Governmental Affairs of the Senate a report on the  
2 effectiveness of the Department’s acquisition processes for  
3 cybersecurity technologies.

4 **TITLE II—PUBLIC-PRIVATE COL-**  
5 **LABORATION ON CYBERSECU-**  
6 **RITY**

7 **SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSE-**  
8 **CURITY.**

9 (a) IN GENERAL.—Subtitle C of title II of the Home-  
10 land Security Act of 2002, as amended by sections 102,  
11 103, 104, 105, 106, and 107, is further amended by add-  
12 ing at the end the following new section:

13 **“SEC. 230B. PUBLIC-PRIVATE COLLABORATION ON CYBER-**  
14 **SECURITY.**

15 “(a) NATIONAL INSTITUTE OF STANDARDS AND  
16 TECHNOLOGY.—The Director of the National Institute of  
17 Standards and Technology, in collaboration with the Sec-  
18 retary, shall, on an ongoing basis, facilitate and support  
19 the development of a voluntary, industry-led set of stand-  
20 ards, guidelines, best practices, methodologies, procedures,  
21 and processes to reduce cyber risks to critical infrastruc-  
22 ture. The Director, in collaboration with the Secretary—

23 “(1) shall—

24 “(A) coordinate closely and continuously  
25 with relevant private entities, critical infrastruc-

1           ture owners and critical infrastructure opera-  
2           tors, Sector Coordinating Councils, Information  
3           Sharing and Analysis Centers, and other rel-  
4           evant industry organizations, and incorporate  
5           industry expertise to the fullest extent possible;

6           “(B) consult with the Sector Specific  
7           Agencies, Federal, State and local governments,  
8           the governments of other countries, and inter-  
9           national organizations;

10          “(C) utilize a prioritized, flexible, repeat-  
11          able, performance-based, and cost-effective ap-  
12          proach, including information security measures  
13          and controls, that may be voluntarily adopted  
14          by critical infrastructure owners and critical in-  
15          frastructure operators to help them identify, as-  
16          sess, and manage cyber risks;

17          “(D) include methodologies to—

18                  “(i) identify and mitigate impacts of  
19                  the cybersecurity measures or controls on  
20                  business confidentiality; and

21                  “(ii) protect individual privacy and  
22                  civil liberties;

23          “(E) incorporate voluntary consensus  
24          standards and industry best practices, and align

1 with voluntary international standards to the  
2 fullest extent possible;

3 “(F) prevent duplication of existing regu-  
4 latory processes and prevent conflict with or su-  
5 perseding of existing regulatory requirements  
6 and processes; and

7 “(G) include such other similar and con-  
8 sistent elements as determined necessary; and

9 “(2) shall not prescribe or otherwise require—

10 “(A) the use of specific solutions;

11 “(B) the use of specific information tech-  
12 nology products or services; or

13 “(C) that information technology products  
14 or services be designed, developed, or manufac-  
15 tured in a particular manner.

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

23 “(1) provide each Sector Coordinating Council  
24 an assessment of the cybersecurity threat to each

1 critical infrastructure sector designated under sec-  
2 tion 227(b), including information relating to—

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

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

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

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

20 “(2) provide recommendations, which may be  
21 voluntarily adopted, on ways to improve cybersecuri-  
22 ty of critical infrastructure.

23 “(c) REPORT.—

24 “(1) IN GENERAL.—Starting 30 days after the  
25 end of the fiscal year in which the National Cyberse-

1 security and Critical Infrastructure Protection Act of  
2 2013 is enacted and annually thereafter, the Sec-  
3 retary shall submit to the Committee on Homeland  
4 Security of the House of Representatives and the  
5 Committee on Homeland Security and Governmental  
6 Affairs of the Senate a report on the state of cyber-  
7 security for each critical infrastructure sector des-  
8 ignated under section 227(b) based on discussions  
9 between the Department and the Sector Coordi-  
10 nating Council in accordance with subsection (b) of  
11 this section. The Secretary shall maintain a public  
12 copy of each report, and each report may include a  
13 non-public annex for proprietary or business-sen-  
14 sitive information. Each report shall include, at a  
15 minimum information relating to—

16 “(A) the risk to each critical infrastructure  
17 sector, including known cyber threats, vulnera-  
18 bilities, and potential consequences;

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

24 “(C) the current status of the voluntary,  
25 industry-led set of standards, guidelines, best

1 practices, methodologies, procedures, and pro-  
2 cesses to reduce cyber risks within each critical  
3 infrastructure sector; and

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

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

21 “(d) LIMITATION.—Information shared with or pro-  
22 vided to the Director of the National Institute of Stand-  
23 ards and Technology or the Secretary for the purpose of  
24 the activities under subsections (a) and (b) shall not be  
25 used by any Federal, State, or local government depart-

1 ment or agency to regulate the activity of any private enti-  
2 ty.”.

3 (b) CLERICAL AMENDMENT.—The table of contents  
4 in section 1(b) of such Act, as amended by sections 102,  
5 103, 104, 105, 106, and 107 is further amended by adding  
6 at the end the following new item:

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

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

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

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

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

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

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

23 (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”; and

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

5 (B) by adding at the end the following new  
6 paragraph:

7 “(7) QUALIFYING CYBER INCIDENT.—

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

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

16 “(i) is unlawful or otherwise exceeds  
17 authorized access authority;

18 “(ii) disrupts or imminently jeopard-  
19 izes the integrity, operation, confiden-  
20 tiality, or availability of programmable  
21 electronic devices, communication net-  
22 works, including hardware, software and  
23 data that are essential to their reliable op-  
24 eration, electronic storage devices, or any  
25 other information system, or the informa-

1 tion that system controls, processes, stores,  
2 or transmits;

3 “(iii) gains access to an information  
4 system or a network of information sys-  
5 tems resulting in—

6 “(I) misappropriation or theft of  
7 data, assets, information, or intellec-  
8 tual property;

9 “(II) corruption of data, assets,  
10 information, or intellectual property;

11 “(III) operational disruption; or

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

16 “(iv) causes harm inside or outside  
17 the United States that results in material  
18 levels of damage, disruption, or casualties  
19 severely affecting the United States popu-  
20 lation, infrastructure, economy, national  
21 morale, or Federal, State, local, or tribal  
22 government functions.”.

23 (b) FUNDING.—Of the amounts authorized to be ap-  
24 propriated for each of fiscal years 2014, 2015, and 2016  
25 for the Science and Technology Directorate of the Depart-

1 ment of Homeland Security, the Secretary of Homeland  
2 Security is authorized to use not less than \$20,000,000  
3 for any such year for the Department's SAFETY Act Of-  
4 fice.

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

6 This Act and the amendments made by this Act do  
7 not—

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

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

15 **SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION**  
16 **OF APPROPRIATIONS.**

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

○