



AMENDMENT NO. \_\_\_\_\_

Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—115th Cong., 2d Sess.****H. R. 3359**

To amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by Mr. JOHNSON (for himself and Mrs.  
McCASKILL)

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity and In-  
5 frastructure Security Agency Act of 2018”.

6 **SEC. 2. CYBERSECURITY AND INFRASTRUCTURE SECURITY**  
7 **AGENCY.**

8 (a) IN GENERAL.—The Homeland Security Act of  
9 2002 (6 U.S.C. 101 et seq.) is amended by adding at the  
10 end the following:

1 **“TITLE XXII—CYBERSECURITY**  
2 **AND INFRASTRUCTURE SECUR-**  
3 **RITY AGENCY**

4 **“Subtitle A—Cybersecurity and**  
5 **Infrastructure Security**

6 **“SEC. 2201. DEFINITIONS.**

7 “In this subtitle:

8 “(1) **CRITICAL INFRASTRUCTURE INFORMA-**  
9 **TION.**—The term ‘critical infrastructure information’  
10 has the meaning given the term in section 2222.

11 “(2) **CYBERSECURITY RISK.**—The term ‘cyber-

12 security risk’ has the meaning given the term in sec-

13 tion 2209.

14 “(3) **CYBERSECURITY THREAT.**—The term ‘cy-

15 bersecurity threat’ has the meaning given the term

16 in section 102(5) of the Cybersecurity Act of 2015

17 (contained in division N of the Consolidated Appro-

18 priations Act, 2016 (Public Law 114–113; 6 U.S.C.

19 1501)).

20 “(4) **NATIONAL CYBERSECURITY ASSET RE-**

21 **SPONSE ACTIVITIES.**—The term ‘national cybersecu-

22 rity asset response activities’ means—

23 “(A) furnishing cybersecurity technical as-

24 sistance to entities affected by cybersecurity

1 risks to protect assets, mitigate vulnerabilities,  
2 and reduce impacts of cyber incidents;

3 “(B) identifying other entities that may be  
4 at risk of an incident and assessing risk to the  
5 same or similar vulnerabilities;

6 “(C) assessing potential cybersecurity risks  
7 to a sector or region, including potential cas-  
8 cading effects, and developing courses of action  
9 to mitigate such risks;

10 “(D) facilitating information sharing and  
11 operational coordination with threat response;  
12 and

13 “(E) providing guidance on how best to  
14 utilize Federal resources and capabilities in a  
15 timely, effective manner to speed recovery from  
16 cybersecurity risks.

17 “(5) SECTOR-SPECIFIC AGENCY.—The term  
18 ‘Sector-Specific Agency’ means a Federal depart-  
19 ment or agency, designated by law or presidential di-  
20 rective, with responsibility for providing institutional  
21 knowledge and specialized expertise of a sector, as  
22 well as leading, facilitating, or supporting programs  
23 and associated activities of its designated critical in-  
24 frastructure sector in the all hazards environment in  
25 coordination with the Department.

1           “(6) SHARING.—The term ‘sharing’ has the  
2           meaning given the term in section 2209.

3   **“SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECU-**  
4           **RITY AGENCY.**

5           “(a) REDESIGNATION.—

6           “(1) IN GENERAL.—The National Protection  
7           and Programs Directorate of the Department shall,  
8           on and after the date of the enactment of this sub-  
9           title, be known as the ‘Cybersecurity and Infrastruc-  
10          ture Security Agency’ (in this subtitle referred to as  
11          the ‘Agency’).

12          “(2) REFERENCES.—Any reference to the Na-  
13          tional Protection and Programs Directorate of the  
14          Department in any law, regulation, map, document,  
15          record, or other paper of the United States shall be  
16          deemed to be a reference to the Cybersecurity and  
17          Infrastructure Security Agency of the Department.

18          “(b) DIRECTOR.—

19          “(1) IN GENERAL.—The Agency shall be head-  
20          ed by a Director of Cybersecurity and Infrastructure  
21          Security (in this subtitle referred to as the ‘Direc-  
22          tor’), who shall report to the Secretary.

23          “(2) REFERENCE.—Any reference to an Under  
24          Secretary responsible for overseeing critical infra-  
25          structure protection, cybersecurity, and any other re-

1       lated program of the Department as described in  
2       section 103(a)(1)(H) as in effect on the day before  
3       the date of enactment of this subtitle in any law,  
4       regulation, map, document, record, or other paper of  
5       the United States shall be deemed to be a reference  
6       to the Director of Cybersecurity and Infrastructure  
7       Security of the Department.

8       “(e) RESPONSIBILITIES.—The Director shall—

9               “(1) lead cybersecurity and critical infrastruc-  
10              ture security programs, operations, and associated  
11              policy for the Agency, including national cybersecu-  
12              rity asset response activities;

13             “(2) coordinate with Federal entities, including  
14              Sector-Specific Agencies, and non-Federal entities,  
15              including international entities, to carry out the cy-  
16              bersecurity and critical infrastructure activities of  
17              the Agency, as appropriate;

18             “(3) carry out the responsibilities of the Sec-  
19              retary to secure Federal information and informa-  
20              tion systems consistent with law, including sub-  
21              chapter II of chapter 35 of title 44, United States  
22              Code, and the Cybersecurity Act of 2015 (contained  
23              in division N of the Consolidated Appropriations  
24              Act, 2016 (Public Law 114–113));

1           “(4) coordinate a national effort to secure and  
2 protect against critical infrastructure risks, con-  
3 sistent with subsection (e)(1)(E);

4           “(5) upon request, provide analyses, expertise,  
5 and other technical assistance to critical infrastruc-  
6 ture owners and operators and, where appropriate,  
7 provide those analyses, expertise, and other technical  
8 assistance in coordination with Sector-Specific Agen-  
9 cies and other Federal departments and agencies;

10           “(6) develop and utilize mechanisms for active  
11 and frequent collaboration between the Agency and  
12 Sector-Specific Agencies to ensure appropriate co-  
13 ordination, situational awareness, and communica-  
14 tions with Sector-Specific Agencies;

15           “(7) maintain and utilize mechanisms for the  
16 regular and ongoing consultation and collaboration  
17 among the Divisions of the Agency to further oper-  
18 ational coordination, integrated situational aware-  
19 ness, and improved integration across the Agency in  
20 accordance with this Act;

21           “(8) develop, coordinate, and implement—

22           “(A) comprehensive strategic plans for the  
23 activities of the Agency; and

24           “(B) risk assessments by and for the  
25 Agency;

1           “(9) carry out emergency communications re-  
2           sponsibilities, in accordance with title XVIII;

3           “(10) carry out cybersecurity, infrastructure se-  
4           curity, and emergency communications stakeholder  
5           outreach and engagement and coordinate that out-  
6           reach and engagement with critical infrastructure  
7           Sector-Specific Agencies, as appropriate; and

8           “(11) carry out such other duties and powers  
9           prescribed by law or delegated by the Secretary.

10          “(d) DEPUTY DIRECTOR.—There shall be in the  
11          Agency a Deputy Director of Cybersecurity and Infra-  
12          structure Security who shall—

13                 “(1) assist the Director in the management of  
14                 the Agency; and

15                 “(2) report to the Director.

16          “(e) CYBERSECURITY AND INFRASTRUCTURE SECU-  
17          RITY AUTHORITIES OF THE SECRETARY.—

18                 “(1) IN GENERAL.—The responsibilities of the  
19                 Secretary relating to cybersecurity and infrastruc-  
20                 ture security shall include the following:

21                         “(A) To access, receive, and analyze law  
22                         enforcement information, intelligence informa-  
23                         tion, and other information from Federal Gov-  
24                         ernment agencies, State, local, tribal, and terri-  
25                         torial government agencies, including law en-

1           forcement agencies, and private sector entities,  
2           and to integrate that information, in support of  
3           the mission responsibilities of the Department,  
4           in order to—

5                   “(i) identify and assess the nature  
6                   and scope of terrorist threats to the home-  
7                   land;

8                   “(ii) detect and identify threats of ter-  
9                   rorism against the United States; and

10                   “(iii) understand those threats in light  
11                   of actual and potential vulnerabilities of  
12                   the homeland.

13                   “(B) To carry out comprehensive assess-  
14                   ments of the vulnerabilities of the key resources  
15                   and critical infrastructure of the United States,  
16                   including the performance of risk assessments  
17                   to determine the risks posed by particular types  
18                   of terrorist attacks within the United States,  
19                   including an assessment of the probability of  
20                   success of those attacks and the feasibility and  
21                   potential efficacy of various countermeasures to  
22                   those attacks. At the discretion of the Sec-  
23                   retary, such assessments may be carried out in  
24                   coordination with Sector-Specific Agencies.



1           “(C) To integrate relevant information,  
2           analysis, and vulnerability assessments, regard-  
3           less of whether the information, analysis, or as-  
4           sessments are provided or produced by the De-  
5           partment, in order to make recommendations,  
6           including prioritization, for protective and sup-  
7           port measures by the Department, other Fed-  
8           eral Government agencies, State, local, tribal,  
9           and territorial government agencies and au-  
10          thorities, the private sector, and other entities  
11          regarding terrorist and other threats to home-  
12          land security.

13          “(D) To ensure, pursuant to section 202,  
14          the timely and efficient access by the Depart-  
15          ment to all information necessary to discharge  
16          the responsibilities under this title, including  
17          obtaining that information from other Federal  
18          Government agencies.

19          “(E) To develop, in coordination with the  
20          Sector-Specific Agencies with available exper-  
21          tise, a comprehensive national plan for securing  
22          the key resources and critical infrastructure of  
23          the United States, including power production,  
24          generation, and distribution systems, informa-  
25          tion technology and telecommunications systems

1 (including satellites), electronic financial and  
2 property record storage and transmission sys-  
3 tems, emergency communications systems, and  
4 the physical and technological assets that sup-  
5 port those systems.

6 “(F) To recommend measures necessary to  
7 protect the key resources and critical infra-  
8 structure of the United States in coordination  
9 with other Federal Government agencies, in-  
10 cluding Sector-Specific Agencies, and in co-  
11 operation with State, local, tribal, and terri-  
12 torial government agencies and authorities, the  
13 private sector, and other entities.

14 “(G) To review, analyze, and make rec-  
15 ommendations for improvements to the policies  
16 and procedures governing the sharing of infor-  
17 mation relating to homeland security within the  
18 Federal Government and between Federal Gov-  
19 ernment agencies and State, local, tribal, and  
20 territorial government agencies and authorities.

21 “(H) To disseminate, as appropriate, infor-  
22 mation analyzed by the Department within the  
23 Department to other Federal Government agen-  
24 cies with responsibilities relating to homeland  
25 security and to State, local, tribal, and terri-

## 11

1           torial government agencies and private sector  
2           entities with those responsibilities in order to  
3           assist in the deterrence, prevention, or preemp-  
4           tion of, or response to, terrorist attacks against  
5           the United States.

6           “(I) To consult with State, local, tribal,  
7           and territorial government agencies and private  
8           sector entities to ensure appropriate exchanges  
9           of information, including law enforcement-re-  
10          lated information, relating to threats of ter-  
11          rorism against the United States.

12          “(J) To ensure that any material received  
13          pursuant to this Act is protected from unau-  
14          thorized disclosure and handled and used only  
15          for the performance of official duties.

16          “(K) To request additional information  
17          from other Federal Government agencies, State,  
18          local, tribal, and territorial government agen-  
19          cies, and the private sector relating to threats  
20          of terrorism in the United States, or relating to  
21          other areas of responsibility assigned by the  
22          Secretary, including the entry into cooperative  
23          agreements through the Secretary to obtain  
24          such information.

1           “(L) To establish and utilize, in conjunc-  
2           tion with the Chief Information Officer of the  
3           Department, a secure communications and in-  
4           formation technology infrastructure, including  
5           data-mining and other advanced analytical  
6           tools, in order to access, receive, and analyze  
7           data and information in furtherance of the re-  
8           sponsibilities under this section, and to dissemi-  
9           nate information acquired and analyzed by the  
10          Department, as appropriate.

11          “(M) To coordinate training and other  
12          support to the elements and personnel of the  
13          Department, other Federal Government agen-  
14          cies, and State, local, tribal, and territorial gov-  
15          ernment agencies that provide information to  
16          the Department, or are consumers of informa-  
17          tion provided by the Department, in order to  
18          facilitate the identification and sharing of infor-  
19          mation revealed in their ordinary duties and the  
20          optimal utilization of information received from  
21          the Department.

22          “(N) To coordinate with Federal, State,  
23          local, tribal, and territorial law enforcement  
24          agencies, and the private sector, as appropriate.

1           “(O) To exercise the authorities and over-  
2           sight of the functions, personnel, assets, and li-  
3           abilities of those components transferred to the  
4           Department pursuant to section 201(g).

5           “(P) To carry out the functions of the na-  
6           tional cybersecurity and communications inte-  
7           gration center under section 2209.

8           “(Q) To carry out the requirements of the  
9           Chemical Facility Anti-Terrorism Standards  
10          Program established under title XXI and the  
11          secure handling of ammonium nitrate program  
12          established under subtitle J of title VIII, or any  
13          successor programs.

14          “(2) REALLOCATION.—The Secretary may re-  
15          allocate within the Agency the functions specified in  
16          sections 2203(b) and 2204(b), consistent with the  
17          responsibilities provided in paragraph (1), upon cer-  
18          tifying to and briefing the appropriate congressional  
19          committees, and making available to the public, at  
20          least 60 days prior to the reallocation that the re-  
21          allocation is necessary for carrying out the activities  
22          of the Agency.

23          “(3) STAFF.—

24                 “(A) IN GENERAL.—The Secretary shall  
25                 provide the Agency with a staff of analysts hav-

1 ing appropriate expertise and experience to as-  
2 sist the Agency in discharging the responsibil-  
3 ities of the Agency under this section.

4 “(B) PRIVATE SECTOR ANALYSTS.—Ana-  
5 lyst under this subsection may include analysts  
6 from the private sector.

7 “(C) SECURITY CLEARANCES.—Analysts  
8 under this subsection shall possess security  
9 clearances appropriate for their work under this  
10 section.

11 “(4) DETAIL OF PERSONNEL.—

12 “(A) IN GENERAL.—In order to assist the  
13 Agency in discharging the responsibilities of the  
14 Agency under this section, personnel of the  
15 Federal agencies described in subparagraph (B)  
16 may be detailed to the Agency for the perform-  
17 ance of analytic functions and related duties.

18 “(B) AGENCIES.—The Federal agencies  
19 described in this subparagraph are—

20 “(i) the Department of State;

21 “(ii) the Central Intelligence Agency;

22 “(iii) the Federal Bureau of Investiga-  
23 tion;

24 “(iv) the National Security Agency;

1                   “(v) the National Geospatial-Intel-  
2                   ligence Agency;

3                   “(vi) the Defense Intelligence Agency;

4                   “(vii) Sector-Specific Agencies; and

5                   “(viii) any other agency of the Fed-  
6                   eral Government that the President con-  
7                   siders appropriate.

8                   “(C) INTERAGENCY AGREEMENTS.—The  
9                   Secretary and the head of a Federal agency de-  
10                  scribed in subparagraph (B) may enter into  
11                  agreements for the purpose of detailing per-  
12                  sonnel under this paragraph.

13                  “(D) BASIS.—The detail of personnel  
14                  under this paragraph may be on a reimbursable  
15                  or non-reimbursable basis.

16                  “(f) COMPOSITION.—The Agency shall be composed  
17                  of the following divisions:

18                  “(1) The Cybersecurity Division, headed by an  
19                  Assistant Director.

20                  “(2) The Infrastructure Security Division,  
21                  headed by an Assistant Director.

22                  “(3) The Emergency Communications Division  
23                  under title XVIII, headed by an Assistant Director.

24                  “(g) CO-LOCATION.—

1           “(1) IN GENERAL.—To the maximum extent  
2           practicable, the Director shall examine the establish-  
3           ment of central locations in geographical regions  
4           with a significant Agency presence.

5           “(2) COORDINATION.—When establishing the  
6           central locations described in paragraph (1), the Di-  
7           rector shall coordinate with component heads and  
8           the Under Secretary for Management to co-locate or  
9           partner on any new real property leases, renewing  
10          any occupancy agreements for existing leases, or  
11          agreeing to extend or newly occupy any Federal  
12          space or new construction.

13          “(h) PRIVACY.—

14                 “(1) IN GENERAL.—There shall be a Privacy  
15                 Officer of the Agency with primary responsibility for  
16                 privacy policy and compliance for the Agency.

17                 “(2) RESPONSIBILITIES.—The responsibilities  
18                 of the Privacy Officer of the Agency shall include—

19                         “(A) assuring that the use of technologies  
20                         by the Agency sustain, and do not erode, pri-  
21                         vacy protections relating to the use, collection,  
22                         and disclosure of personal information;

23                         “(B) assuring that personal information  
24                         contained in systems of records of the Agency  
25                         is handled in full compliance as specified in sec-



1           tion 552a of title 5, United States Code (com-  
2           monly known as the ‘Privacy Act of 1974’);

3           “(C) evaluating legislative and regulatory  
4           proposals involving collection, use, and disclo-  
5           sure of personal information by the Agency;  
6           and

7           “(D) conducting a privacy impact assess-  
8           ment of proposed rules of the Agency on the  
9           privacy of personal information, including the  
10          type of personal information collected and the  
11          number of people affected.

12          “(i) SAVINGS.—Nothing in this title may be con-  
13          strued as affecting in any manner the authority, existing  
14          on the day before the date of enactment of this title, of  
15          any other component of the Department or any other Fed-  
16          eral department or agency.

17          **“SEC. 2203. CYBERSECURITY DIVISION.**

18          “(a) ESTABLISHMENT.—

19                  “(1) IN GENERAL.—There is established in the  
20          Agency a Cybersecurity Division.

21                  “(2) ASSISTANT DIRECTOR.—The Cybersecurity  
22          Division shall be headed by an Assistant Director for  
23          Cybersecurity (in this section referred to as the ‘As-  
24          sistant Director’), who shall—

1           “(A) be at the level of Assistant Secretary  
2           within the Department;

3           “(B) be appointed by the President with-  
4           out the advice and consent of the Senate; and

5           “(C) report to the Director.

6           “(3) REFERENCE.—Any reference to the Assist-  
7           ant Secretary for Cybersecurity and Communica-  
8           tions in any law, regulation, map, document, record,  
9           or other paper of the United States shall be deemed  
10          to be a reference to the Assistant Director for Cy-  
11          bersecurity.

12          “(b) FUNCTIONS.—The Assistant Director shall—

13           “(1) direct the cybersecurity efforts of the  
14          Agency;

15           “(2) carry out activities, at the direction of the  
16          Director, related to the security of Federal informa-  
17          tion and Federal information systems consistent  
18          with law, including subchapter II of chapter 35 of  
19          title 44, United States Code, and the Cybersecurity  
20          Act of 2015 (contained in division N of the Consoli-  
21          dated Appropriations Act, 2016 (Public Law 114-  
22          113));

23           “(3) fully participate in the mechanisms re-  
24          quired under section 2202(c)(6); and

1           “(4) carry out such other duties and powers as  
2           prescribed by the Director.

3   **“SEC. 2204. INFRASTRUCTURE SECURITY DIVISION.**

4           “(a) ESTABLISHMENT.—

5           “(1) IN GENERAL.—There is established in the  
6           Agency an Infrastructure Security Division.

7           “(2) ASSISTANT DIRECTOR.—The Infrastruc-  
8           ture Security Division shall be headed by an Assist-  
9           ant Director for Infrastructure Security (in this sec-  
10          tion referred to as the ‘Assistant Director’), who  
11          shall—

12                  “(A) be at the level of Assistant Secretary  
13                  within the Department;

14                  “(B) be appointed by the President with-  
15                  out the advice and consent of the Senate; and

16                  “(C) report to the Director.

17           “(3) REFERENCE.—Any reference to the Assist-  
18           ant Secretary for Infrastructure Protection in any  
19           law, regulation, map, document, record, or other  
20           paper of the United States shall be deemed to be a  
21           reference to the Assistant Director for Infrastruc-  
22           ture Security.

23           “(b) FUNCTIONS.—The Assistant Director shall—

24                  “(1) direct the critical infrastructure security  
25                  efforts of the Agency;

1           “(2) carry out, at the direction of the Director,  
2           the Chemical Facilities Anti-Terrorism Standards  
3           Program established under title XXI and the secure  
4           handling of ammonium nitrate program established  
5           under subtitle J of title VIII, or any successor pro-  
6           grams;

7           “(3) fully participate in the mechanisms re-  
8           quired under section 2202(c)(6); and

9           “(4) carry out such other duties and powers as  
10          prescribed by the Director.”

11          (b) TREATMENT OF CERTAIN POSITIONS.—

12           (1) UNDER SECRETARY.—The individual serv-  
13          ing as the Under Secretary appointed pursuant to  
14          section 103(a)(1)(H) of the Homeland Security Act  
15          of 2002 (6 U.S.C. 113(a)(1)) of the Department of  
16          Homeland Security on the day before the date of en-  
17          actment of this Act may continue to serve as the Di-  
18          rector of Cybersecurity and Infrastructure Security  
19          of the Department on and after such date.

20           (2) DIRECTOR FOR EMERGENCY COMMUNICA-  
21          TIONS.—The individual serving as the Director for  
22          Emergency Communications of the Department of  
23          Homeland Security on the day before the date of en-  
24          actment of this Act may continue to serve as the As-

1       assistant Director for Emergency Communications of  
2       the Department on and after such date.

3               (3) ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The individual serving  
4       as the Assistant Secretary for Cybersecurity and  
5       Communications on the day before the date of enact-  
6       ment of this Act may continue to serve as the As-  
7       sistant Director for Cybersecurity on and after such  
8       date.  
9

10              (4) ASSISTANT SECRETARY FOR INFRASTRUC-  
11       TURE PROTECTION.—The individual serving as the  
12       Assistant Secretary for Infrastructure Protection on  
13       the day before the date of enactment of this Act may  
14       continue to serve as the Assistant Director for Infra-  
15       structure Security on and after such date.

16       (c) REFERENCE.—Any reference to—

17              (1) the Office of Emergency Communications in  
18       any law, regulation, map, document, record, or other  
19       paper of the United States shall be deemed to be a  
20       reference to the Emergency Communications Divi-  
21       sion; and

22              (2) the Director for Emergency Communica-  
23       tions in any law, regulation, map, document, record,  
24       or other paper of the United States shall be deemed

1 to be a reference to the Assistant Director for Emer-  
2 gency Communications.

3 (d) OVERSIGHT.—The Director of Cybersecurity and  
4 Infrastructure Security of the Department of Homeland  
5 Security shall provide to Congress, in accordance with the  
6 deadlines specified in paragraphs (1) through (6), infor-  
7 mation on the following:

8 (1) Not later than 60 days after the date of en-  
9 actment of this Act, a briefing on the activities of  
10 the Agency relating to the development and use of  
11 the mechanisms required pursuant to section  
12 2202(c)(6) of the Homeland Security Act of 2002  
13 (as added by subsection (a)).

14 (2) Not later than 1 year after the date of the  
15 enactment of this Act, a briefing on the activities of  
16 the Agency relating to the use and improvement by  
17 the Agency of the mechanisms required pursuant to  
18 section 2202(c)(6) of the Homeland Security Act of  
19 2002 and how such activities have impacted coordi-  
20 nation, situational awareness, and communications  
21 with Sector-Specific Agencies.

22 (3) Not later than 90 days after the date of the  
23 enactment of this Act, information on the mecha-  
24 nisms of the Agency for regular and ongoing con-  
25 sultation and collaboration, as required pursuant to

1 section 2202(e)(7) of the Homeland Security Act of  
2 2002 (as added by subsection (a)).

3 (4) Not later than 1 year after the date of the  
4 enactment of this Act, information on the activities  
5 of the consultation and collaboration mechanisms of  
6 the Agency as required pursuant to section  
7 2202(e)(7) of the Homeland Security Act of 2002,  
8 and how such mechanisms have impacted oper-  
9 ational coordination, situational awareness, and inte-  
10 gration across the Agency.

11 (5) Not later than 180 days after the date of  
12 enactment of this Act, information, which shall be  
13 made publicly available and updated as appropriate,  
14 on the mechanisms and structures of the Agency re-  
15 sponsible for stakeholder outreach and engagement,  
16 as required under section 2202(e)(10) of the Home-  
17 land Security Act of 2002 (as added by subsection  
18 (a)).

19 (e) CYBER WORKFORCE.—Not later than 90 days  
20 after the date of enactment of this Act, the Director of  
21 the Cybersecurity and Infrastructure Security Agency of  
22 the Department of Homeland Security, in coordination  
23 with the Director of the Office of Personnel Management,  
24 shall submit to Congress a report detailing how the Agen-  
25 cy is meeting legislative requirements under the Cyberse-

1 ecurity Workforce Assessment Act (Public Law 113–246;  
2 128 Stat. 2880) and the Homeland Security Cybersecurity  
3 Workforce Assessment Act (enacted as section 4 of the  
4 Border Patrol Agent Pay Reform Act of 2014; Public Law  
5 113–277) to address cyber-workforce needs.

6 (f) FACILITY.—Not later than 180 days after the  
7 date of enactment of this Act, the Director of the Cyberse-  
8 curity and Infrastructure Security Agency of the Depart-  
9 ment of Homeland Security shall report to Congress on  
10 the most efficient and effective methods of consolidating  
11 Agency facilities, personnel, and programs to most effec-  
12 tively carry out the Agency’s mission.

13 (g) TECHNICAL AND CONFORMING AMENDMENTS TO  
14 THE HOMELAND SECURITY ACT OF 2002.—The Home-  
15 land Security Act of 2002 (6 U.S.C. 101 et seq.) is amend-  
16 ed—

17 (1) by amending section 103(a)(1)(H) (6  
18 U.S.C. 113(a)(1)(H)) to read as follows:

19 “(H) A Director of the Cybersecurity and  
20 Infrastructure Security Agency.”;

21 (2) in title II (6 U.S.C. 121 et seq.)—

22 (A) in the title heading, by striking “**AND**  
23 **INFRASTRUCTURE PROTECTION**”;

24 (B) in the subtitle A heading, by striking  
25 “**and Infrastructure Protection**”;



- 1 (C) in section 201 (6 U.S.C. 121)—
- 2 (i) in the section heading, by striking
- 3 **“AND INFRASTRUCTURE PROTEC-**
- 4 **TION”**;
- 5 (ii) in subsection (a)—
- 6 (I) in the subsection heading, by
- 7 striking **“AND INFRASTRUCTURE PRO-**
- 8 **TECTION”**; and
- 9 (II) by striking **“and an Office of**
- 10 **Infrastructure Protection”**;
- 11 (iii) in subsection (b)—
- 12 (I) in the subsection heading, by
- 13 striking **“AND ASSISTANT SECRETARY**
- 14 **FOR INFRASTRUCTURE PROTECTION”**;
- 15 and
- 16 (II) by striking paragraph (3);
- 17 (iv) in subsection (c)—
- 18 (I) by striking **“and infrastruc-**
- 19 **ture protection”**; and
- 20 (II) by striking **“or the Assistant**
- 21 **Secretary for Infrastructure Protec-**
- 22 **tion, as appropriate”**;
- 23 (v) in subsection (d)—

1 (I) in the subsection heading, by  
2 striking “AND INFRASTRUCTURE PRO-  
3 TECTION”;

4 (II) in the matter preceding  
5 paragraph (1), by striking “and infra-  
6 structure protection”;

7 (III) by striking paragraphs (5),  
8 (6), and (25);

9 (IV) by redesignating paragraphs  
10 (7) through (24) as paragraphs (5)  
11 through (22), respectively;

12 (V) by redesignating paragraph  
13 (26) as paragraph (23); and

14 (VI) in paragraph (23)(B)(i), as  
15 so redesignated, by striking “section  
16 319” and inserting “section 320”;

17 (vi) in subsection (e)(1), by striking  
18 “and the Office of Infrastructure Protec-  
19 tion”; and

20 (vii) in subsection (f)(1), by striking  
21 “and the Office of Infrastructure Protec-  
22 tion”;

23 (D) in section 202 (6 U.S.C. 122)—

24 (i) in subsection (c), in the matter  
25 preceding paragraph (1), by striking “Di-

1 rector of Central Intelligence” and insert-  
2 ing “Director of National Intelligence”;  
3 and

4 (ii) in subsection (d)(2), by striking  
5 “Director of Central Intelligence” and in-  
6 serting “Director of National Intelligence”;  
7 (E) in section 204 (6 U.S.C. 124a)—

8 (i) in subsection (c)(1), in the matter  
9 preceding subparagraph (A), by striking  
10 “Assistant Secretary for Infrastructure  
11 Protection” and inserting “Director of the  
12 Cybersecurity and Infrastructure Security  
13 Agency”; and

14 (ii) in subsection (d)(1), in the matter  
15 preceding subparagraph (A), by striking  
16 “Assistant Secretary for Infrastructure  
17 Protection” and inserting “Director of the  
18 Cybersecurity and Infrastructure Security  
19 Agency”;

20 (F) in section 210A(c)(2)(B) (6 U.S.C.  
21 124h(c)(2)(B)), by striking “Office of Infra-  
22 structure Protection” and inserting “Cybersecu-  
23 rity and Infrastructure Security Agency”;

24 (G) by redesignating section 210E (6  
25 U.S.C. 124i) as section 2214 and transferring

1 such section to appear after section 2213 (as  
2 redesignated by subparagraph (I));

3 (H) in subtitle B, by redesignating sections  
4 211 through 215 (6 U.S.C. 101 note, and 131  
5 through 134) as sections 2221 through 2225,  
6 respectively, and transferring such subtitle, in-  
7 cluding the enumerator and heading of subtitle  
8 B and such sections, to appear after section  
9 2214 (as redesignated by subparagraph (G));

10 (I) by redesignating sections 223 through  
11 230 (6 U.S.C. 143 through 151) as sections  
12 2205 through 2213, respectively, and transfer-  
13 ring such sections to appear after section 2204,  
14 as added by this Act;

15 (J) by redesignating section 210F as sec-  
16 tion 210E; and

17 (K) by redesignating subtitles C and D as  
18 subtitles B and C, respectively;

19 (3) in title III (6 U.S.C. 181 et seq.)—

20 (A) in section 302 (6 U.S.C. 182)—

21 (i) by striking “biological,” each  
22 place that term appears and inserting “bi-  
23 ological,”; and

24 (ii) in paragraph (3), by striking “As-  
25 sistant Secretary for Infrastructure Protec-

1           tion” and inserting “Director of the Cyber-  
2           security and Infrastructure Security Agen-  
3           cy”;

4           (B) by redesignating the second section  
5           319 (6 U.S.C. 195f) (relating to EMP and  
6           GMD mitigation research and development) as  
7           section 320; and

8           (C) in section 320(c)(1), as so redesign-  
9           ated, by striking “Section 214” and inserting  
10          “Section 2224”;

11          (4) in title V (6 U.S.C. 311 et seq.)—

12           (A) in section 508(d)(2)(D) (6 U.S.C.  
13           318(d)(2)(D)), by striking “The Director of the  
14           Office of Emergency Communications of the  
15           Department of Homeland Security” and insert-  
16           ing “The Assistant Director for Emergency  
17           Communications”;

18           (B) in section 514 (6 U.S.C. 321e)—

19           (i) by striking subsection (b); and

20           (ii) by redesignating subsection (c) as  
21           subsection (b); and

22           (C) in section 523 (6 U.S.C. 321i)—

23           (i) in subsection (a), in the matter  
24           preceding paragraph (1), by striking “As-  
25           sistant Secretary for Infrastructure Protec-

1                   tion” and inserting “Director of Cyberse-  
2                   curity and Infrastructure Security”; and

3                   (ii) in subsection (c), by striking “As-  
4                   sistant Secretary for Infrastructure Protec-  
5                   tion” and inserting “Director of Cyberse-  
6                   curity and Infrastructure Security”;

7                   (5) in title VIII (6 U.S.C. 361 et seq.)—

8                   (A) in section 884(d)(4)(A)(ii) (6 U.S.C.  
9                   464(d)(4)(A)(ii)), by striking “Under Secretary  
10                  responsible for overseeing critical infrastructure  
11                  protection, cybersecurity, and other related pro-  
12                  grams of the Department” and inserting “Di-  
13                  rector of Cybersecurity and Infrastructure Se-  
14                  curity”; and

15                  (B) in section 899B(a) (6 U.S.C. 488a(a)),  
16                  by adding at the end the following: “Such regu-  
17                  lations shall be carried out by the Cybersecurity  
18                  and Infrastructure Security Agency.”;

19                  (6) in title XVIII (6 U.S.C. 571 et seq.)—

20                  (A) in section 1801 (6 U.S.C. 571)—

21                   (i) in the section heading, by striking  
22                   “**OFFICE OF EMERGENCY COMMU-**  
23                   **NICATIONS**” and inserting “**EMERGENCY**  
24                   **COMMUNICATIONS DIVISION**”;

25                   (ii) in subsection (a)—

1 (I) by striking “Office of Emer-  
2 gency Communications” and inserting  
3 “Emergency Communications Divi-  
4 sion”; and

5 (II) by adding at the end the fol-  
6 lowing: “The Division shall be located  
7 in the Cybersecurity and Infrastruc-  
8 ture Security Agency.”;

9 (iii) by amending subsection (b) to  
10 read as follows:

11 “(b) ASSISTANT DIRECTOR.—The head of the Divi-  
12 sion shall be the Assistant Director for Emergency Com-  
13 munications. The Assistant Director shall report to the  
14 Director of Cybersecurity and Infrastructure Security. All  
15 decisions of the Assistant Director that entail the exercise  
16 of significant authority shall be subject to the approval  
17 of the Director of Cybersecurity and Infrastructure Secu-  
18 rity.”;

19 (iv) in subsection (c)—

20 (I) in the matter preceding para-  
21 graph (1), by inserting “Assistant”  
22 before “Director”;

23 (II) in paragraph (15), as added  
24 by section 1431(a)(7), by striking  
25 “and” at the end;

1 (III) by redesignating paragraph  
2 (16), as so redesignated by section  
3 1431(a)(3), as paragraph (17); and  
4 (IV) by inserting after paragraph  
5 (15) the following:

6 “(16) fully participate in the mechanisms re-  
7 quired under section 2202(c)(8); and”;

8 (v) in subsection (d), in the matter  
9 preceding paragraph (1), by inserting “As-  
10 sistant” before “Director”; and

11 (vi) in subsection (e), in the matter  
12 preceding paragraph (1), by inserting “As-  
13 sistant” before “Director”;

14 (B) in sections 1802 through 1805 (6  
15 U.S.C. 572 through 575), by striking “Director  
16 for Emergency Communications” each place  
17 that term appears and inserting “Assistant Di-  
18 rector for Emergency Communications”;

19 (C) in section 1809 (6 U.S.C. 579)—

20 (i) by striking “Director of Emer-  
21 gency Communications” each place that  
22 term appears and inserting “Assistant Di-  
23 rector for Emergency Communications”;

24 (ii) in subsection (b)—



1 (I) by striking “Director for  
2 Emergency Communications” and in-  
3 serting “Assistant Director for Emer-  
4 gency Communications”; and

5 (II) by striking “Office of Emer-  
6 gency Communications” and inserting  
7 “Emergency Communications Divi-  
8 sion”;

9 (iii) in subsection (e)(3), by striking  
10 “the Director” and inserting “the Assist-  
11 ant Director”; and

12 (iv) in subsection (m)(1)—

13 (I) by striking “The Director”  
14 and inserting “The Assistant Direc-  
15 tor”;

16 (II) by striking “the Director de-  
17 termines” and inserting “the Assist-  
18 ant Director determines”; and

19 (III) by striking “Office of Emer-  
20 gency Communications” and inserting  
21 “Cybersecurity and Infrastructure Se-  
22 curity Agency”;

23 (D) in section 1810 (6 U.S.C. 580)—

24 (i) in subsection (a)(1), by striking  
25 “Director of the Office of Emergency Com-

1           communications (referred to in this section as  
2           the ‘Director’)” and inserting “Assistant  
3           Director for Emergency Communications  
4           (referred to in this section as the ‘Assist-  
5           ant Director’)”;

6           (ii) in subsection (c), by striking “Of-  
7           fice of Emergency Communications” and  
8           inserting “Emergency Communications Di-  
9           vision”; and

10          (iii) by striking “Director” each place  
11          that term appears and inserting “Assistant  
12          Director”;

13          (7) in title XX (6 U.S.C. 601 et seq.)—

14           (A) in paragraph (5)(A)(iii)(II) of section  
15           2001 (6 U.S.C. 601), as so redesignated by sec-  
16           tion 1451(b), by striking “section 210E(a)(2)”  
17           and inserting “section 2214(a)(2)”;

18           (B) in section 2008(a)(3) (6 U.S.C.  
19           609(a)(3)), by striking “section 210E(a)(2)”  
20           and inserting “section 2214(a)(2)”;

21           (C) in section 2021 (6 U.S.C. 611)—

22           (i) by striking subsection (c); and

23           (ii) by redesignating subsection (d) as  
24           subsection (e);

25          (8) in title XXI (6 U.S.C. 621 et seq.)—

1 (A) in section 2102(a)(1) (6 U.S.C.  
2 622(a)(1)), by inserting “, which shall be lo-  
3 cated in the Cybersecurity and Infrastructure  
4 Security Agency” before the period at the end;  
5 and

6 (B) in section 2104(c)(2) (6 U.S.C.  
7 624(c)(2)), by striking “Under Secretary re-  
8 sponsible for overseeing critical infrastructure  
9 protection, cybersecurity, and other related pro-  
10 grams of the Department appointed under sec-  
11 tion 103(a)(1)(H)” and inserting “Director of  
12 Cybersecurity and Infrastructure Security”; and  
13 (9) in title XXII, as added by this Act—

14 (A) in subtitle A—

15 (i) in section 2205, as so redesign-  
16 nated—

17 (I) in the matter preceding para-  
18 graph (1)—

19 (aa) by striking “section  
20 201” and inserting “section  
21 2202”; and

22 (bb) by striking “Under Sec-  
23 retary appointed under section  
24 103(a)(1)(H)” and inserting “Di-

1 rector of Cybersecurity and In-  
2 frastructure Security”; and

3 (II) in paragraph (1)(B), by  
4 striking “and” at the end;

5 (ii) in section 2206, as so redesign-  
6 nated, by striking “Assistant Secretary for  
7 Infrastructure Protection” and inserting  
8 “Director of Cybersecurity and Infrastruc-  
9 ture Security”;

10 (iii) in section 2209, as so redesign-  
11 nated—

12 (I) by striking “Under Secretary  
13 appointed under section  
14 103(a)(1)(H)” each place that term  
15 appears and inserting “Director”;

16 (II) in subsection (a)(4), by  
17 striking “section 212(5)” and insert-  
18 ing “section 2222(5)”;

19 (III) in subsection (b), by adding  
20 at the end the following: “The Center  
21 shall be located in the Cybersecurity  
22 and Infrastructure Security Agency.  
23 The head of the Center shall report to  
24 the Assistant Director for Cybersecu-  
25 rity.”; and

1 (IV) in subsection (c)(11), by  
2 striking “Office of Emergency Com-  
3 munications” and inserting “Emer-  
4 gency Communications Division”;

5 (iv) in section 2210, as so redesign-  
6 nated—

7 (I) by striking “section 227”  
8 each place that term appears and in-  
9 serting “section 2209”; and

10 (II) in subsection (c)—

11 (aa) by striking “Under Sec-  
12 retary appointed under section  
13 103(a)(1)(H)” and inserting “Di-  
14 rector of Cybersecurity and In-  
15 frastructure Security”; and

16 (bb) by striking “section  
17 212(5)” and inserting “section  
18 2222(5)”;

19 (v) in section 2211, as so redesign-  
20 nated—

21 (I) in subsection (b)(2)(A), by  
22 striking “the section 227” and insert-  
23 ing “section 2209”; and

1 (II) in subsection (c)(1)(C), by  
2 striking “section 707” and inserting  
3 “section 706”;

4 (vi) in section 2212, as so redesign-  
5 nated, by striking “section 212(5)” and in-  
6 serting “section 2222(5)”;

7 (vii) in section 2213(a), as so redesign-  
8 nated—

9 (I) in paragraph (3), by striking  
10 “section 228” and inserting “section  
11 2210”; and

12 (II) in paragraph (4), by striking  
13 “section 227” and inserting “section  
14 2209”; and

15 (viii) in section 2214, as so redesign-  
16 nated—

17 (I) by striking subsection (e);  
18 and

19 (II) by redesignating subsection  
20 (f) as subsection (e); and

21 (B) in subtitle B—

22 (i) in section 2222(8), as so redesign-  
23 nated, by striking “section 227” and in-  
24 serting “section 2209”; and

1 (ii) in section 2224(h), as so redesignated,  
2 nated, by striking “section 213” and in-  
3 serting “section 2223”;

4 (h) TECHNICAL AND CONFORMING AMENDMENTS TO  
5 OTHER LAWS.—

6 (1) CYBERSECURITY ACT OF 2015.—The Cyber-  
7 security Act of 2015 (6 U.S.C. 1501 et seq.) is  
8 amended—

9 (A) in section 202(2) (6 U.S.C. 131  
10 note)—

11 (i) by striking “section 227” and in-  
12 serting “section 2209”; and

13 (ii) by striking “, as so redesignated  
14 by section 223(a)(3) of this division”;

15 (B) in section 207(2) (Public Law 114-  
16 113; 129 Stat. 2962)—

17 (i) by striking “section 227” and in-  
18 serting “section 2209”; and

19 (ii) by striking “, as redesignated by  
20 section 223(a) of this division,”;

21 (C) in section 208 (Public Law 114-113;  
22 129 Stat. 2962), by striking “Under Secretary  
23 appointed under section 103(a)(1)(H) of the  
24 Homeland Security Act of 2002 (6 U.S.C.  
25 113(a)(1)(H))” and inserting “Director of Cy-

1 bersecurity and Infrastructure Security of the  
2 Department”;

3 (D) in section 222 (6 U.S.C. 1521)—

4 (i) in paragraph (2)—

5 (I) by striking “section 228” and  
6 inserting “section 2210”; and

7 (II) by striking “, as added by  
8 section 223(a)(4) of this division”;  
9 and

10 (ii) in paragraph (4)—

11 (I) by striking “section 227” and  
12 inserting “section 2209”; and

13 (II) by striking “, as so redesign-  
14 dated by section 223(a)(3) of this di-  
15 vision”;

16 (E) in section 223(b) (6 U.S.C. 151  
17 note)—

18 (i) by striking “section 230(b)(1) of  
19 the Homeland Security Act of 2002, as  
20 added by subsection (a)” each place that  
21 term appears and inserting “section  
22 2213(b)(1) of the Homeland Security Act  
23 of 2002”; and

24 (ii) in paragraph (1)(B), by striking  
25 “section 230(b)(2) of the Homeland Secu-



1 rity Act of 2002, as added by subsection  
2 (a)” and inserting “section 2213(b)(2) of  
3 the Homeland Security Act of 2002”;  
4 (F) in section 226 (6 U.S.C. 1524)—  
5 (i) in subsection (a)—  
6 (I) in paragraph (1)—  
7 (aa) by striking “section  
8 230” and inserting “section  
9 2213”; and  
10 (bb) by striking “, as added  
11 by section 223(a)(6) of this divi-  
12 sion”;  
13 (II) in paragraph (4)—  
14 (aa) by striking “section  
15 228(b)(1)” and inserting “section  
16 2210(b)(1)”; and  
17 (bb) by striking “, as added  
18 by section 223(a)(4) of this divi-  
19 sion”; and  
20 (III) in paragraph (5)—  
21 (aa) by striking “section  
22 230(b)” and inserting “section  
23 2213(b)”; and

1 (bb) by striking “, as added  
2 by section 223(a)(6) of this divi-  
3 sion”; and

4 (ii) in subsection (c)(1)(A)(vi)—

5 (I) by striking “section  
6 230(c)(5)” and inserting “section  
7 2213(c)(5)”; and

8 (II) by striking “, as added by  
9 section 223(a)(6) of this division”;

10 (G) in section 227 (6 U.S.C. 1525)—

11 (i) in subsection (a)—

12 (I) by striking “section 230” and  
13 inserting “section 2213”; and

14 (II) by striking “, as added by  
15 section 223(a)(6) of this division,”;  
16 and

17 (ii) in subsection (b)—

18 (I) by striking “section  
19 230(d)(2)” and inserting “section  
20 2213(d)(2)”; and

21 (II) by striking “, as added by  
22 section 223(a)(6) of this division,”;  
23 and

24 (H) in section 404 (6 U.S.C. 1532)—

1 (i) by striking “Director for Emer-  
2 gency Communications” each place that  
3 term appears and inserting “Assistant Di-  
4 rector for Emergency Communications”;  
5 and

6 (ii) in subsection (a)—

7 (I) by striking “section 227” and  
8 inserting “section 2209”; and

9 (II) by striking “, as redesign-  
10 nated by section 223(a)(3) of this di-  
11 vision,”.

12 (2) SMALL BUSINESS ACT.—Section  
13 21(a)(8)(B) of the Small Business Act (15 U.S.C.  
14 648(a)(8)(B)) is amended by striking “section  
15 227(a) of the Homeland Security Act of 2002 (6  
16 U.S.C. 148(a))” and inserting “section 2209(a) of  
17 the Homeland Security Act of 2002”.

18 (3) TITLE 5.—Subchapter II of chapter 53 of  
19 title 5, United States Code, is amended—

20 (A) in section 5314, by inserting after  
21 “Under Secretaries, Department of Homeland  
22 Security.” the following:

23 “Director, Cybersecurity and Infrastructure Se-  
24 curity Agency.”; and

1 (B) in section 5315, by inserting after  
2 “Assistant Secretaries, Department of Home-  
3 land Security.” the following:

4 “Assistant Director for Cybersecurity, Cyberse-  
5 curity and Infrastructure Security Agency.

6 “Assistant Director for Infrastructure Security,  
7 Cybersecurity and Infrastructure Security Agency.”.

8 (i) TABLE OF CONTENTS AMENDMENTS.—The table  
9 of contents in section 1(b) of the Homeland Security Act  
10 of 2002 (Public Law 107–296; 116 Stat. 2135) is amend-  
11 ed—

12 (1) by striking the item relating to title II and  
13 inserting the following:

“TITLE II—INFORMATION ANALYSIS”;

14 (2) by striking the item relating to subtitle A  
15 of title II and inserting the following:

“Subtitle A—Information and Analysis; Access to Information”;

16 (3) by striking the item relating to section 201  
17 and inserting the following:

“Sec. 201. Information and analysis.”;

18 (4) by striking the items relating to sections  
19 210E and 210F and inserting the following:

“Sec. 210E. Classified Information Advisory Officer.”;

20 (5) by striking the items relating to subtitle B  
21 of title II and sections 211 through 215;

1 (6) by striking the items relating to section 223  
2 through section 230;

3 (7) by striking the item relating to subtitle C  
4 and inserting the following:

“Subtitle B—Information Security”;

5 (8) by striking the item relating to subtitle D  
6 and inserting the following:

“Subtitle C—Office of Science and Technology”;

7 (9) by striking the items relating to sections  
8 317, 319, 318, and 319 and inserting the following:

“Sec. 317. Promoting antiterrorism through international cooperation program.

“Sec. 318. Social media working group.

“Sec. 319. Transparency in research and development.

“Sec. 320. EMP and GMD mitigation research and development.”;

9 (10) by striking the item relating to section  
10 1801 and inserting the following:

“Sec. 1801. Emergency Communications Division.”; and

11 (11) by adding at the end the following:

“TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY  
AGENCY

“Subtitle A—Cybersecurity and Infrastructure Security

“Sec. 2201. Definitions.

“Sec. 2202. Cybersecurity and Infrastructure Security Agency.

“Sec. 2203. Cybersecurity Division.

“Sec. 2204. Infrastructure Security Division.

“Sec. 2205. Enhancement of Federal and non-Federal cybersecurity.

“Sec. 2206. Net guard.

“Sec. 2207. Cyber Security Enhancement Act of 2002.

“Sec. 2208. Cybersecurity recruitment and retention.

“Sec. 2209. National cybersecurity and communications integration center.

“Sec. 2210. Cybersecurity plans.

“Sec. 2211. Cybersecurity strategy.

“Sec. 2212. Clearances.

“Sec. 2213. Federal intrusion detection and prevention system.

“Sec. 2214. National Asset Database.

“Subtitle B—Critical Infrastructure Information

"Sec. 2221. Short title.

"Sec. 2222. Definitions.

"Sec. 2223. Designation of critical infrastructure protection program.

"Sec. 2224. Protection of voluntarily shared critical infrastructure information.

"Sec. 2225. No private right of action."

1 **SEC. 3. TRANSFER OF OTHER ENTITIES.**

2 (a) **OFFICE OF BIOMETRIC IDENTITY MANAGE-**  
3 **MENT.**—The Office of Biometric Identity Management of  
4 the Department of Homeland Security located in the Na-  
5 tional Protection and Programs Directorate of the Depart-  
6 ment of Homeland Security on the day before the date  
7 of enactment of this Act is hereby transferred to the Man-  
8 agement Directorate of the Department.

9 (b) **FEDERAL PROTECTIVE SERVICE.**—

10 (1) **IN GENERAL.**—Not later than 90 days after  
11 the completion of the Government Accountability Of-  
12 fice review of the organizational placement of the  
13 Federal Protective Service (authorized under section  
14 1315 of title 40, United States Code), the Secretary  
15 of Homeland Security shall determine the appro-  
16 priate placement of the Service within the Depart-  
17 ment of Homeland Security and commence the  
18 transfer of the Service to such component, direc-  
19 torate, or other office of the Department that the  
20 Secretary so determines appropriate.

21 (2) **EXCEPTION.**—If the Secretary of Homeland  
22 Security determines pursuant to paragraph (1) that  
23 no component, directorate, or other office of the De-

1       partment of Homeland Security is an appropriate  
2       placement for the Federal Protective Service, the  
3       Secretary shall—

4               (A) provide to the Committee on Home-  
5       land Security and the Committee on Transpor-  
6       tation and Infrastructure of the House of Rep-  
7       resentatives and the Committee on Homeland  
8       Security and Governmental Affairs of the Sen-  
9       ate and the Office of Management and Budget  
10      a detailed explanation, in writing, of the reason  
11      for such determination that includes—

12              (i) information on how the Depart-  
13      ment considered the Government Account-  
14      ability Office review described in such  
15      paragraph;

16              (ii) a list of the components, direc-  
17      torates, or other offices of the Department  
18      that were considered for such placement;  
19      and

20              (iii) information on why each such  
21      component, directorate, or other office of  
22      the Department was determined to not be  
23      an appropriate placement for the Service;

24              (B) not later than 120 days after the com-  
25      pletion of the Government Accountability Office

1 review described in such paragraph, develop and  
2 submit to the committees specified in subpara-  
3 graph (A) and the Office of Management and  
4 Budget a plan to coordinate with other appro-  
5 priate Federal agencies, including the General  
6 Services Administration, to determine a more  
7 appropriate placement for the Service; and

8 (C) not later than 180 days after the com-  
9 pletion of such Government Accountability Of-  
10 fice review, submit to such committees and the  
11 Office of Management and Budget a rec-  
12 ommendation regarding the appropriate place-  
13 ment of the Service within the executive branch  
14 of the Federal Government.

15 **SEC. 4. DHS REPORT ON CLOUD-BASED CYBERSECURITY.**

16 (a) **DEFINITION.**—In this section, the term “Depart-  
17 ment” means the Department of Homeland Security.

18 (b) **REPORT.**—Not later than 120 days after the date  
19 of enactment of this Act, the Secretary of Homeland Secu-  
20 rity, in coordination with the Director of the Office of  
21 Management and Budget and the Administrator of Gen-  
22 eral Services, shall submit to the Committee on Homeland  
23 Security and Governmental Affairs of the Senate and the  
24 Committee on Oversight and Government Reform and the  
25 Committee on Homeland Security of the House of Rep-



1 representatives a report on the leadership role of the Depart-  
2 ment in cloud-based cybersecurity deployments for civilian  
3 Federal departments and agencies, which shall include—

4 (1) information on the plan of the Department  
5 for ensuring access to a security operations center as  
6 a service capability in accordance with the December  
7 19, 2017 Report to the President on Federal IT  
8 Modernization issued by the American Technology  
9 Council;

10 (2) information on what service capabilities  
11 under paragraph (1) the Department will prioritize,  
12 including—

13 (A) criteria the Department will use to  
14 evaluate capabilities offered by the private sec-  
15 tor; and

16 (B) how Federal government- and private  
17 sector-provided capabilities will be integrated to  
18 enable visibility and consistency of such capa-  
19 bilities across all cloud and on premise environ-  
20 ments, as called for in the report described in  
21 paragraph (1); and

22 (3) information on how the Department will  
23 adapt the current capabilities of, and future en-  
24 hancements to, the intrusion detection and preven-  
25 tion system of the Department and the Continuous

1       Diagnostics and Mitigation Program of the Depart-  
2       ment to secure civilian Federal government networks  
3       in a cloud environment.

4       **SEC. 5. RULE OF CONSTRUCTION.**

5       Nothing in this Act or an amendment made by this  
6       Act may be construed as—

7               (1) conferring new authorities to the Secretary  
8       of Homeland Security, including programmatic, reg-  
9       ulatory, or enforcement authorities, outside of the  
10      authorities in existence on the day before the date  
11      of enactment of this Act;

12              (2) reducing or limiting the programmatic, reg-  
13      ulatory, or enforcement authority vested in any  
14      other Federal agency by statute; or

15              (3) affecting in any manner the authority, exist-  
16      ing on the day before the date of enactment of this  
17      Act, of any other Federal agency or component of  
18      the Department of Homeland Security.

19      **SEC. 6. PROHIBITION ON ADDITIONAL FUNDING.**

20      No additional funds are authorized to be appro-  
21      priated to carry out this Act or the amendments made  
22      by this Act. This Act and the amendments made by this  
23      Act shall be carried out using amounts otherwise author-  
24      ized.