

115TH CONGRESS
1ST SESSION

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.

IN THE HOUSE OF REPRESENTATIVES

JULY 24, 2017

Mr. MCCAUL (for himself, Mr. THOMPSON of Mississippi, Mr. RATCLIFFE, Mr. RICHMOND, Mr. KATKO, Mr. HURD, Mr. DONOVAN, Mr. GALLAGHER, Mr. HIGGINS of Louisiana, Mr. GARRETT, and Mr. FITZPATRICK) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Energy and Commerce, Oversight and Government Reform, and Transportation and Infrastructure, 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 authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, 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 “Cybersecurity and In-
5 frastructure Security Agency Act of 2017”.

1 **SEC. 2. CYBERSECURITY AND INFRASTRUCTURE SECURITY**
2 **AGENCY.**

3 (a) IN GENERAL.—The Homeland Security Act of
4 2002 is amended by adding at the end the following new
5 title:

6 **“TITLE XXII—CYBERSECURITY**
7 **AND INFRASTRUCTURE SECU-**
8 **RITY AGENCY**

9 **“Subtitle A—Cybersecurity and**
10 **Infrastructure Security**

11 **“SEC. 2201. DEFINITIONS.**

12 “In this subtitle:

13 “(1) CRITICAL INFRASTRUCTURE INFORMA-
14 TION.—The term ‘critical infrastructure information’
15 has the meaning given such term in section 2215.

16 “(2) CRITICAL INFRASTRUCTURE RISK.—The
17 term ‘critical infrastructure risk’ means threats to
18 and vulnerabilities of critical infrastructure and any
19 related consequences, including consequences caused
20 by or resulting from an act of terrorism.

21 “(3) CYBERSECURITY RISK.—The term ‘cyber-
22 security risk’ has the meaning given such term in
23 section 2209.

24 “(4) CYBERSECURITY THREAT.—The term ‘cy-
25 bersecurity threat’ has the meaning given such term
26 in paragraph (5) of section 102 of the Cybersecurity

1 Act of 2015 (contained in division N of the Consoli-
2 dated Appropriations Act, 2016 (Public Law 114–
3 113; 6 U.S.C. 1501)).

4 “(5) FEDERAL ENTITY.—The term ‘Federal en-
5 tity’ has the meaning given such term in paragraph
6 (8) of section 102 of the Cybersecurity Act of 2015
7 (contained in division N of the Consolidated Appro-
8 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
9 1501)).

10 “(6) NON-FEDERAL ENTITY.—The term ‘non-
11 Federal entity’ has the meaning given such term in
12 paragraph (14) of section 102 of the Cybersecurity
13 Act of 2015 (contained in division N of the Consoli-
14 dated Appropriations Act, 2016 (Public Law 114–
15 113; 6 U.S.C. 1501)).

16 “(7) SHARING.—The term ‘sharing’ has the
17 meaning given such term in section 2209.

18 “(8) NATIONAL CYBERSECURITY ASSET RE-
19 SPONSE ACTIVITIES.—The term ‘national cybersecu-
20 rity asset response activities’ means—

21 “(A) furnishing technical assistance to en-
22 tities affected by cybersecurity risks to protect
23 assets, mitigate vulnerabilities, and reduce im-
24 pacts of cyber incidents;

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

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

8 “(D) facilitating information sharing and
9 operational coordination with threat response;
10 and

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

15 **“SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECU-**
16 **RITY AGENCY.**

17 “(a) REDESIGNATION.—

18 “(1) IN GENERAL.—The National Protection
19 and Programs Directorate of the Department shall,
20 on and after the date of the enactment of this sub-
21 title, be known as the ‘Cybersecurity and Infrastruc-
22 ture Security Agency’ (in this subtitle referred to as
23 the ‘Agency’).

24 “(2) REFERENCES.—Any reference to the Na-
25 tional Protection and Programs Directorate of the

1 Department in any law, regulation, map, document,
2 record, or other paper of the United States shall be
3 deemed to be a reference to the Cybersecurity and
4 Infrastructure Security Agency of the Department.

5 “(b) DIRECTOR.—

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

10 “(2) REFERENCE.—Any reference to an Under
11 Secretary responsible for overseeing critical infra-
12 structure protection, cybersecurity, and any other re-
13 lated program of the Department as described in
14 section 103(a)(1)(H) as in effect on the day before
15 the date of the enactment of this subtitle in any law,
16 regulation, map, document, record, or other paper of
17 the United States shall be deemed to be a reference
18 to the Director of Cybersecurity and Infrastructure
19 Security of the Department.

20 “(c) RESPONSIBILITIES.—The Director shall—

21 “(1) lead cybersecurity and critical infrastruc-
22 ture security programs, operations, and associated
23 policy for the Agency, including national cybersecu-
24 rity asset response activities;

1 “(2) coordinate with Federal entities and non-
2 Federal entities, including international entities, to
3 carry out the cybersecurity and critical infrastruc-
4 ture activities of the Agency, as appropriate;

5 “(3) carry out the Secretary’s responsibilities to
6 secure Federal information and information systems
7 consistent with law, including subchapter II of chap-
8 ter 35 of title 44, United States Code, and the Cy-
9 bersecurity Act of 2015 (contained in division N of
10 the Consolidated Appropriations Act, 2016 (Public
11 Law 114–113));

12 “(4) coordinate a national effort to secure and
13 protect against critical infrastructure risks;

14 “(5) upon request provide analyses, expertise,
15 and other technical assistance to critical infrastruc-
16 ture owners and operators and, where appropriate,
17 provide such analyses, expertise, and other technical
18 assistance in coordination with critical infrastructure
19 sector specific agencies and other Federal depart-
20 ments and agencies;

21 “(6) to the extent required by law, exercise du-
22 ties in coordination with sector-specific agencies;

23 “(7) maintain and utilize mechanisms for the
24 regular and ongoing consultation and collaboration
25 among the Agency’s Divisions to further operational

1 coordination, integrated situational awareness, and
2 improved integration across the Agency in accord-
3 ance with this Act;

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

5 “(A) comprehensive strategic plans for the
6 activities of the Agency; and

7 “(B) risk assessments;

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

10 “(10) carry out cybersecurity, infrastructure se-
11 curity, and emergency communications stakeholder
12 outreach and engagement; and

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

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

18 “(1) assist the Director in the management of
19 the Agency; and

20 “(2) report to the Director.

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

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

1 “(A) To access, receive, and analyze law
2 enforcement information, intelligence informa-
3 tion, and other information from Federal Gov-
4 ernment agencies, State, local, tribal, and terri-
5 torial government agencies (including law en-
6 forcement agencies), and private sector entities,
7 and to integrate such information, in support of
8 the mission responsibilities of the Department,
9 in order to—

10 “(i) identify and assess the nature
11 and scope of terrorist threats to the home-
12 land;

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

15 “(iii) understand such threats in light
16 of actual and potential vulnerabilities of
17 the homeland.

18 “(B) To carry out comprehensive assess-
19 ments of the vulnerabilities of the key resources
20 and critical infrastructure of the United States,
21 including the performance of risk assessments
22 to determine the risks posed by particular types
23 of terrorist attacks within the United States
24 (including an assessment of the probability of
25 success of such attacks and the feasibility and

1 potential efficacy of various countermeasures to
2 such attacks).

3 “(C) To integrate relevant information,
4 analysis, and vulnerability assessments (regard-
5 less of whether such information, analysis, or
6 assessments are provided or produced by the
7 Department) in order to identify priorities for
8 protective and support measures by the Depart-
9 ment, other Federal Government agencies,
10 State, local, tribal, and territorial government
11 agencies and authorities, the private sector, and
12 other entities regarding terrorist and other
13 threats to homeland security.

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

20 “(E) To develop a comprehensive national
21 plan for securing the key resources and critical
22 infrastructure of the United States, including
23 power production, generation, and distribution
24 systems, information technology and tele-
25 communications systems (including satellites),

1 electronic financial and property record storage
2 and transmission systems, emergency prepared-
3 ness communications systems, and the physical
4 and technological assets that support such sys-
5 tems.

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 and in
10 cooperation with State, local, tribal, and terri-
11 torial government agencies and authorities, the
12 private sector, and other entities.

13 “(G) To review, analyze, and make rec-
14 ommendations for improvements to the policies
15 and procedures governing the sharing of law en-
16 forcement information, and other information
17 relating to homeland security within the Fed-
18 eral Government and between Federal Govern-
19 ment agencies and State, local, tribal, and terri-
20 torial 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
24 agencies with responsibilities relating to home-
25 land security, and to State, local, tribal, and

1 territorial government agencies and private sec-
2 tor entities with such responsibilities in order to
3 assist in the deterrence, prevention, preemption
4 of, or response to, terrorist attacks against the
5 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 ensure, in conjunction with the
12 chief information officer of the Department,
13 that any information databases and analytical
14 tools developed or utilized by the Department—

15 “(i) are compatible with one another
16 and with relevant information databases of
17 other Federal Government agencies; and

18 “(ii) treat information in such data-
19 bases in a manner that complies with ap-
20 plicable Federal law on privacy.

21 “(N) To coordinate training and other sup-
22 port to the elements and personnel of the De-
23 partment, other Federal Government agencies,
24 and State, local, tribal, and territorial govern-
25 ment agencies that provide information to the

1 Department, or are consumers of information
2 provided by the Department, in order to facili-
3 tate the identification and sharing of informa-
4 tion revealed in their ordinary duties and the
5 optimal utilization of information received from
6 the Department.

7 “(O) To coordinate with Federal, State,
8 local, tribal, and territorial law enforcement
9 agencies, and the private sector, as appropriate.

10 “(P) To exercise the authorities and over-
11 sight of the functions, personnel, assets, and li-
12 abilities of those components transferred to the
13 Department pursuant to section 201(g).

14 “(Q) To carry out the functions of the na-
15 tional cybersecurity and communications inte-
16 gration center under section 2209.

17 “(R) To carry out requirements of the
18 Chemical Facilities Anti-Terrorism Standards
19 Program established under title XXI and the
20 secure handling of ammonium nitrate estab-
21 lished under subtitle J of title VIII.

22 “(2) MODIFICATION.—The Secretary may mod-
23 ify the functions specified in sections 2203(b) and
24 2204(b) upon certifying to the Committee on Home-
25 land Security of the House of Representatives and

1 the Committee on Homeland Security and Govern-
2 mental Affairs of the Senate 60 days prior to any
3 such modification that such modification is nec-
4 essary for carrying out the activities of the Agency.

5 “(3) STAFF.—

6 “(A) IN GENERAL.—The Secretary shall
7 provide the Agency with a staff of analysts hav-
8 ing appropriate expertise and experience to as-
9 sist the Agency in discharging its responsibil-
10 ities under this section.

11 “(B) PRIVATE SECTOR ANALYSTS.—Ana-
12 lysts under this subsection may include analysts
13 from the private sector.

14 “(C) SECURITY CLEARANCES.—Analysts
15 under this subsection shall possess security
16 clearances appropriate for their work under this
17 section.

18 “(4) DETAIL OF PERSONNEL.—

19 “(A) IN GENERAL.—In order to assist the
20 Agency in discharging its responsibilities under
21 this section, personnel of the Federal agencies
22 referred to in subparagraph (B) may be de-
23 tailed to the Agency for the performance of
24 analytic functions and related duties.

1 “(B) AGENCIES SPECIFIED.—The Federal
2 agencies referred to in subparagraph (A) are
3 the following:

4 “(i) The Department of State.

5 “(ii) The Central Intelligence Agency.

6 “(iii) The Federal Bureau of Inves-
7 tigation.

8 “(iv) The National Security Agency.

9 “(v) The National Geospatial-Intel-
10 ligence Agency.

11 “(vi) The Defense Intelligence Agen-
12 cy.

13 “(vii) Any other agency of the Federal
14 Government that the President considers
15 appropriate.

16 “(C) INTERAGENCY AGREEMENTS.—The
17 Secretary and the head of an agency specified
18 in subparagraph (B) may enter into agreements
19 for the purpose of detailing personnel under
20 this paragraph.

21 “(D) BASIS.—The detail of personnel
22 under this paragraph may be on a reimbursable
23 or non-reimbursable basis.

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

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

3 “(2) The Infrastructure Security Division,
4 headed by an Assistant Director.

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

7 “(g) CO-LOCATION.—To the maximum extent prac-
8 ticable, the Director shall examine the establishment of
9 central locations in geographical regions with a significant
10 Agency presence. When establishing such locations, the
11 Director shall coordinate with component heads and the
12 Under Secretary for Management to co-locate or partner
13 on any new real property leases, renewing any existing
14 leases, or agreeing to extend or newly occupy any Federal
15 space or new construction.

16 “(h) PRIVACY.—

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

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

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

1 “(B) assuring that personal information
2 contained in Privacy Act systems of records of
3 the Agency is handled in full compliance with
4 fair information practices as specified in the
5 Privacy Act of 1974;

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

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

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

20 **“SEC. 2203. CYBERSECURITY DIVISION.**

21 “(a) ESTABLISHMENT.—

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

24 “(2) ASSISTANT DIRECTOR.—The Cybersecurity
25 Division shall be headed by an Assistant Director for

1 Cybersecurity (in this subtitle referred to as the ‘As-
2 sistant Director’), who shall—

3 “(A) be at the level of Assistant Secretary
4 within the Department; and

5 “(B) 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 information and
17 information systems for Federal entities 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 subsection (c)(7) of section 2202; 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 of 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; and

14 “(B) report to the Director.

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

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

22 “(1) direct the critical infrastructure security
23 efforts of the Agency;

24 “(2) carry out efforts, at the direction of the
25 Director, to secure the United States high-risk

1 chemicals and chemical facilities consistent with law,
2 including the Chemical Facilities Anti-Terrorism
3 Standards Program established under title XXI and
4 the secure handling of ammonium nitrate established
5 under subtitle J of title VIII;

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

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

10 (b) TREATMENT OF CERTAIN POSITIONS.—

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

1 Assistant Director for Emergency Communications
2 of 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 the
6 enactment of this Act may continue to serve as the
7 Assistant Director for Cybersecurity on and after
8 such date.

10 (4) ASSISTANT SECRETARY FOR INFRASTRUCTURE SECURITY.—The individual serving as the As-
11 sistant Secretary for Infrastructure Protection on
12 the day before the date of the enactment of this Act
13 may continue to serve as the Assistant Director for
14 Infrastructure 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 the Cybersecurity
4 and Infrastructure Security Agency of the Department of
5 Homeland Security shall provide to Congress, in accord-
6 ance with the deadlines specified in paragraphs (1) and
7 (2), information on the following:

8 (1) Not later than 90 days after the date of the
9 enactment of this Act, information on the Agency’s
10 mechanisms for regular and ongoing consultation
11 and collaboration, as required pursuant to section
12 2202(c)(7) of the Homeland Security Act of 2002
13 (as added by this Act).

14 (2) Not later than one year after the date of
15 the enactment of this Act, the activities of the Agen-
16 cy’s consultation and collaboration mechanisms and
17 how such mechanisms have impacted operational co-
18 ordination, situational awareness, and integration
19 across the Agency.

20 (e) CYBER WORKFORCE.—Not later than 90 days
21 after the date of the enactment of this subtitle, the Direc-
22 tor of the Cybersecurity and Infrastructure Security Agen-
23 cy of the Department of Homeland Security shall submit
24 to Congress a report detailing how the Agency is meeting
25 legislative requirements under the Cybersecurity Work-

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

6 (f) FACILITY.—Not later than 180 days after the
 7 date of the enactment of this Act, the Director of the Cy-
 8 bersecurity and Infrastructure Security Agency of the De-
 9 partment of Homeland Security shall report to Congress
 10 on the most efficient and effective methods of consoli-
 11 dating Agency facilities, personnel, and programs to most
 12 effectively carry out the Agency’s mission.

13 (g) CONFORMING AMENDMENTS TO THE HOMELAND
 14 SECURITY ACT OF 2002.—The Homeland Security Act of
 15 2002 is amended—

16 (1) in title I, by amending subparagraph (H) of
 17 section 103(a)(1) (6 U.S.C. 113(a)(1)) to read as
 18 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 heading, by striking

7 **“AND INFRASTRUCTURE PROTEC-**
8 **TION”**; and

9 (II) by striking **“and an Office of**
10 **Infrastructure Protection”**;

11 (iii) in subsection (b)—

12 (I) in the heading, by striking

13 **“AND ASSISTANT SECRETARY FOR IN-**
14 **FRASTRUCTURE PROTECTION”**; and

15 (II) by striking paragraph (3);

16 (iv) in subsection (c)—

17 (I) by striking **“and infrastruc-**
18 **ture protection”**; and

19 (II) by striking **“or the Assistant**
20 **Secretary for Infrastructure Protec-**
21 **tion, as appropriate”**;

22 (v) in subsection (d)—

23 (I) in the heading, by striking

24 **“AND INFRASTRUCTURE PROTEC-**
25 **TION”**;

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

4 (III) by striking paragraphs (5)
5 and (6) and redesignating paragraphs
6 (7) through (26) as paragraphs (5)
7 through (24), respectively;

8 (IV) by striking paragraph (23),
9 as so redesignated; and

10 (V) by redesignating paragraph
11 (24), as so redesignated, as paragraph
12 (23);

13 (vi) in subsection (e)(1), by striking
14 “and the Office of Infrastructure Protec-
15 tion”; and

16 (vii) in subsection (f)(1), by striking
17 “and the Office of Infrastructure Protec-
18 tion”;

19 (D) in section 204 (6 U.S.C. 124a)—

20 (i) in subsection (c)(1), in the matter
21 preceding subparagraph (A), by striking
22 “Assistant Secretary for Infrastructure
23 Protection” and inserting “Director of the
24 Cybersecurity and Infrastructure Security
25 Agency”; and

1 (ii) in subsection (d)(1), in the matter
2 preceding subparagraph (A), by striking
3 “Assistant Secretary for Infrastructure
4 Protection” and inserting “Director of the
5 Cybersecurity and Infrastructure Security
6 Agency”;

7 (E) in subparagraph (B) of section
8 210A(c)(2) (6 U.S.C. 124h(c)(2)), by striking
9 “Office of Infrastructure Protection” and in-
10 serting “Cybersecurity and Infrastructure Secu-
11 rity Agency”;

12 (F) by transferring section 210E (6 U.S.C.
13 124) to appear after section 2212 (as redesign-
14 ated by subparagraph (G) of this paragraph)
15 and redesignating such section 210E as section
16 2214;

17 (G) in subtitle B, by redesignating sections
18 211 through 215 (6 U.S.C. 101 note through
19 134) as sections 2221 through 2225, respec-
20 tively, and inserting such redesignated sections,
21 including the enumerator and heading of sub-
22 title B (containing such redesignated sections),
23 after section 2213, as redesignated by subpara-
24 graph (E) of this paragraph; and

1 (H) by redesignating sections 223 through
2 230 (6 U.S.C. 143 through 151) as sections
3 2205 through 2213, respectively, and inserting
4 such redesignated sections after section 2204,
5 as added by this Act;

6 (3) in title III, in paragraph (3) of section 302
7 (6 U.S.C. 182), by striking “Assistant Secretary for
8 Infrastructure Protection” and inserting “Director
9 of the Cybersecurity and Infrastructure Security
10 Agency”;

11 (4) in title V—

12 (A) in section 514 (6 U.S.C. 321(c)), by—

13 (i) striking subsection (b); and

14 (ii) redesignating subsection (c) as
15 subsection (b);

16 (B) in section 523 (6 U.S.C. 321I)—

17 (i) in subsection (a), in the matter
18 preceding paragraph (1), by striking “As-
19 sistant Secretary for Infrastructure Protec-
20 tion” and inserting “Director of the Cyber-
21 security and Infrastructure Security Agen-
22 cy”; and

23 (ii) in subsection (c), by striking “As-
24 sistant Secretary for Infrastructure Protec-
25 tion” and inserting “Director of the Cyber-

1 security and Infrastructure Security Agen-
 2 cy”; and

3 (C) in section 524(a)(2)(B) (6 U.S.C.
 4 321m(a)(2)(B)), in the matter preceding clause
 5 (i)—

6 (i) by striking “Assistant Secretary
 7 for Infrastructure Protection” and insert-
 8 ing “Director of the Cybersecurity and In-
 9 frastructure Security Agency”; and

10 (ii) by striking “of the Assistant Sec-
 11 retary” and inserting “of the Director”;

12 (5) in title VIII, in section 899B(a) (6 U.S.C.
 13 488a(a)), by inserting at the end the following new
 14 sentence: “Such regulations shall be carried out by
 15 the Cybersecurity and Infrastructure Security Agen-
 16 cy.”;

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

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

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

23 (ii) in subsection (a)—

24 (I) by striking “Office of Emer-
 25 gency Communications” and inserting

1 “Emergency Communications Divi-
2 sion”; and

3 (II) by adding at the end the fol-
4 lowing new sentence: “The Division
5 shall be located in the Cybersecurity
6 and Infrastructure Security Agency.”;
7 (iii) in subsection (b)—

8 (I) in the first sentence, by in-
9 serting “Assistant” before “Director”;
10 and

11 (II) in the second sentence, by
12 striking “Assistant Secretary for Cy-
13 bersecurity and Communications” and
14 inserting “Director of the Cybersecu-
15 rity and Infrastructure Security Agen-
16 cy”;
17 (iv) in subsection (c)—

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

21 (II) in paragraph (14), by strik-
22 ing “and” at the end;

23 (III) by redesignating paragraph
24 (15) as paragraph (16); and

1 (IV) by inserting after paragraph
2 (14) the following new paragraph:

3 “(15) fully participate in the mechanisms re-
4 quired under subsection (c)(7) of section 2202;
5 and”;

6 (v) in subsection (d), by inserting
7 “Assistant” before “Director”; and

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

11 (B) in sections 1802 through 1805 (6
12 U.S.C. 575), by striking “Director for Emer-
13 gency Communications” each place it appears
14 and inserting “Assistant Director for Emer-
15 gency Communications”;

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

17 (i) by striking “Director for Emer-
18 gency Communications” and inserting “As-
19 sistant Director for Emergency Commu-
20 nications”; and

21 (ii) by striking “Office of Emergency
22 Communications” each place it appears
23 and inserting “Emergency Communica-
24 tions Division”; and

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

1 (i) in subsection (a)(1), by striking
 2 “Director of the Office of Emergency Com-
 3 munications (referred to in this section as
 4 the ‘Director’)” and inserting “Assistant
 5 Director for the Emergency Communica-
 6 tions Division (referred to in this section
 7 as the ‘Assistant Director’)”;

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

12 (iii) by striking “Director” each place
 13 it appears and inserting “Assistant Direc-
 14 tor”;

15 (7) in title XXI (6 U.S.C. 621 et seq.)—

16 (A) in section 2101 (6 U.S.C. 621)—

17 (i) by redesignating paragraphs (4)
 18 through (14) as paragraphs (5) through
 19 (15), respectively; and

20 (ii) by inserting after paragraph (3)
 21 the following new paragraph:

22 “(4) the term ‘Director’ means the Director of
 23 the Cybersecurity and Infrastructure Security Agen-
 24 cy;”;

1 (B) in paragraph (1) of section 2102(a) (6
2 U.S.C. 622(a)), by inserting at the end the fol-
3 lowing new sentence: “Such Program shall be
4 located in the Cybersecurity and Infrastructure
5 Security Agency.”; and

6 (C) in paragraph (2) of section 2104(c) (6
7 U.S.C. 624(c)), by striking “Under Secretary
8 responsible 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 the Cybersecurity and Infrastructure Security
13 Agency”; and

14 (8) in title XXII, as added by this Act—

15 (A) in section 2205, as so redesignated, in
16 the matter preceding paragraph (1), by striking
17 “Under Secretary appointed under section
18 103(a)(1)(H)” and inserting “Director of the
19 Cybersecurity and Infrastructure Security
20 Agency”;

21 (B) in section 2206, as so redesignated, by
22 striking “Assistant Secretary for Infrastructure
23 Protection” and inserting “Director of the Cy-
24 bersecurity and Infrastructure Security Agen-
25 cy”;

1 (C) in section 2209, as so redesignated—

2 (i) by striking “Under Secretary ap-
3 pointed under section 103(a)(1)(H)” each
4 place it appears and inserting “Director of
5 the Cybersecurity and Infrastructure Secu-
6 rity Agency”;

7 (ii) in subsection (b), by adding at the
8 end the following new sentences: “The
9 Center shall be located in the Cybersecu-
10 rity and Infrastructure Security Agency.
11 The head of the Center shall report to the
12 Assistant Director for Cybersecurity.”; and

13 (iii) in subsection (c)(11), by striking
14 “Office of Emergency Communications”
15 and inserting “Emergency Communica-
16 tions Division”;

17 (D) in section 2210, as so redesignated—

18 (i) by striking “section 227” each
19 place it appears and inserting “section
20 2209”; and

21 (ii) in subsection (c), by striking
22 “Under Secretary appointed under section
23 103(a)(1)(H)” and inserting “Director of
24 the Cybersecurity and Infrastructure Secu-
25 rity Agency”;

1 (E) in section 2211, as so redesignated, by
 2 striking “section 212(5)” and inserting “section
 3 2215(5)”; and

4 (F) in section 2212, as so redesignated, in
 5 subsection (a)—

6 (i) in paragraph (3), by striking “sec-
 7 tion 228” and inserting “section 2210”;
 8 and

9 (ii) in paragraph (4), by striking “sec-
 10 tion 227” and inserting “section 2209”.

11 (h) CONFORMING AMENDMENT TO TITLE 5, UNITED
 12 STATES CODE.—Section 5314 of title 5, United States
 13 Code, is amended by inserting after “Under Secretaries,
 14 Department of Homeland Security.” the following new
 15 item:

16 “Director, Cybersecurity and Infrastructure Se-
 17 curity Agency.”.

18 (i) CLERICAL AMENDMENTS.—The table of contents
 19 in section 1(b) of the Homeland Security Act of 2002 is
 20 amended—

21 (1) in title II—

22 (A) in the item relating to the title head-
 23 ing, by striking “**AND INFRASTRUC-**
 24 **TURE PROTECTION**”;

1 (B) in the item relating to the heading of
 2 subtitle A, by striking “**and Infrastructure**
 3 **Protection**”;

4 (C) in the item relating to section 201, by
 5 striking “**AND INFRASTRUCTURE PROTEC-**
 6 **TION**”;

7 (D) by striking the item relating to section
 8 210E;

9 (E) by striking the items relating to sub-
 10 title B of title II; and

11 (F) by striking the items relating to sec-
 12 tion 223 through section 230; and

13 (2) by adding at the end the following new
 14 items:

“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. Cybersecurity 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 the enactment of this Act is hereby transferred to the
8 Management Directorate of the Department.

9 (b) FEDERAL PROTECTIVE SERVICE.—The Secretary
10 of Homeland Security is authorized to transfer the Fed-
11 eral Protective Service, as authorized under section 1315
12 of title 40, United States Code, to any component, direc-
13 torate, or other office of the Department of Homeland Se-
14 curity that the Secretary determines appropriate.

15 **SEC. 4. RULE OF CONSTRUCTION.**

16 Nothing in this Act may be construed as—

17 (1) conferring new authorities to the Secretary
18 of Homeland Security, including programmatic, reg-
19 ulatory, or enforcement authorities, outside of the
20 authorities in existence on the day before the date
21 of the enactment of this Act;

22 (2) reducing or limiting the programmatic, reg-
23 ulatory, or enforcement authority vested in any
24 other Federal agency by statute; or

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

5 **SEC. 5. PROHIBITION ON ADDITIONAL FUNDING.**

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

○