

114TH CONGRESS
2D SESSION

H. R. 5390

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 7, 2016

Mr. McCAUL (for himself, Mr. RATCLIFFE, and Ms. JACKSON LEE) 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 Protection 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 Protection Agency Act of 2016”.

1 **SEC. 2. CYBERSECURITY AND INFRASTRUCTURE PROTEC-**
2 **TION 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 PRO-**
8 **TECTION AGENCY**

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

11 **“SEC. 2201. DEFINITIONS.**

12 “In this subtitle—

13 “(1) CRITICAL INFRASTRUCTURE INCIDENT.—
14 The term ‘critical infrastructure incident’ means an
15 occurrence that actually or immediately jeopardizes,
16 without lawful authority, the integrity, confiden-
17 tially, or availability of critical infrastructure.

18 “(2) CRITICAL INFRASTRUCTURE INFORMA-
19 TION.—The term ‘critical infrastructure information’
20 has the meaning given such term in section 2215.

21 “(3) CRITICAL INFRASTRUCTURE RISK.—The
22 term ‘critical infrastructure risk’ means threats to
23 and vulnerabilities of critical infrastructure and any
24 related consequences caused by or resulting from un-
25 authorized access, use, disclosure, degradation, dis-
26 ruption, modification, or destruction of such critical

1 infrastructure, including such related consequences
2 caused by an act of terrorism.

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

6 “(5) CYBERSECURITY THREAT.—The term ‘cy-
7 bersecurity threat’ has the meaning given such term
8 in paragraph (5) of section 102 of the Cybersecurity
9 Information Sharing Act of 2015 (contained in divi-
10 sion N of the Consolidated Appropriations Act, 2016
11 (Public Law 114–113; 6 U.S.C. 1501)).

12 “(6) FEDERAL ENTITY.—The term ‘Federal en-
13 tity’ has the meaning given such term in paragraph
14 (8) of section 102 of the Cybersecurity Information
15 Sharing Act of 2015 (contained in division N of the
16 Consolidated Appropriations Act, 2016 (Public Law
17 114–113; 6 U.S.C. 1501)).

18 “(7) NON-FEDERAL ENTITY.—The term ‘non-
19 Federal entity’ has the meaning given such term in
20 paragraph (14) of section 102 of the Cybersecurity
21 Information Sharing Act of 2015 (contained in divi-
22 sion N of the Consolidated Appropriations Act, 2016
23 (Public Law 114–113; 6 U.S.C. 1501)).

24 “(8) SHARING.—The term ‘sharing’ has the
25 meaning given such term in section 2209.

1 **“SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE PRO-**
2 **TECTION AGENCY.**

3 “(a) REDESIGNATION.—

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

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

16 “(b) MISSION.—The mission of the Agency shall be
17 to lead national efforts to protect and enhance the security
18 and resilience of the cyber and critical infrastructure of
19 the United States.

20 “(c) DIRECTOR.—

21 “(1) IN GENERAL.—The Agency shall be head-
22 ed by a Director of National Cybersecurity (in this
23 subtitle referred to as the ‘Director’).

24 “(2) REFERENCE.—Any reference to an Under
25 Secretary responsible for overseeing critical infra-
26 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 the 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 National Cybersecurity of the De-
7 partment.

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

9 “(1) lead cybersecurity and critical infrastruc-
10 ture protection policy and operations for the Depart-
11 ment;

12 “(2) serve as the primary representative of the
13 Department for coordinating with Federal entities,
14 non-Federal entities, and international partners the
15 cybersecurity and critical infrastructure protection
16 policy and operations referred to in paragraph (1);

17 “(3) facilitate a national effort to strengthen
18 and maintain secure, functioning, and resilient crit-
19 ical infrastructure from threats;

20 “(4) maintain and utilize mechanisms, includ-
21 ing a coordinating body for the regular and ongoing
22 consultation and collaboration among the Agency’s
23 Divisions to further operation coordination, inte-
24 grated situational awareness, and improved integra-
25 tion across the Agency;

1 “(5) develop, coordinate, and implement—

2 “(A) comprehensive strategic plans for cy-
3 bersecurity and critical infrastructure protec-
4 tion; and

5 “(B) risk assessments for the Department,
6 in accordance with subsection (f);

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

9 “(7) carry out the authorities designated to the
10 Secretary under section 1315 of title 40 United
11 States Code; and

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

14 “(e) RISK ASSESSMENTS.—

15 “(1) NATIONAL RISK ASSESSMENTS.—The Di-
16 rector, in coordination with the heads of relevant
17 components of the Department and other appro-
18 priate Federal entities, shall develop, coordinate, and
19 update periodically (not less often than once every
20 two years) a national risk assessment of—

21 “(A) cybersecurity risks; and

22 “(B) critical infrastructure risks.

23 “(2) INTEGRATED NATIONAL RISK ASSESS-
24 MENTS.—The Director shall develop, coordinate, and
25 update periodically (not less often than once every

1 two years) an integrated national risk assessment
2 that assesses all of the cybersecurity risks and crit-
3 ical infrastructure risks referred to in paragraph (1)
4 and compares each such risk and incident against
5 one another according to their relative risk, includ-
6 ing cascading effects between each such risk.

7 “(3) INCLUSION IN ASSESSMENTS.—Each na-
8 tional risk assessment required under paragraph (1)
9 and integrated national risk assessment required
10 under paragraph (2) shall include—

11 “(A) a description of the data and method-
12 ology used for each such assessment; and

13 “(B) if applicable, actions or counter-meas-
14 ures recommended or taken by the Secretary or
15 the head of another Federal agency to address
16 issues identified in each such assessment.

17 “(4) CLASSIFICATION.—The Director shall en-
18 sure that each national risk assessment required
19 under paragraph (1) and integrated national risk as-
20 sessment required under paragraph (2) has a classi-
21 fied and unclassified version.

22 “(5) PROVISION TO CONGRESS.—The Director
23 shall provide to the Committee on Homeland Secu-
24 rity of the House of Representatives and the Com-
25 mittee on Homeland Security and Governmental Af-

1 fairs of the Senate each national risk assessment re-
2 quired under paragraph (1) and integrated national
3 risk assessment required under paragraph (2) not
4 later than 30 days after the completion of each such
5 assessment.

6 “(f) **METHODOLOGY.**—In developing each national
7 risk assessment required under subsection (f)(1) and inte-
8 grated national risk assessment required under subsection
9 (g)(2), the Director, in consultation with the heads of rel-
10 evant Federal entities, shall—

11 “(1) assess the proposed methodology to be
12 used for such assessments; and

13 “(2) consider the evolving threat to the United
14 States as indicated by the intelligence community
15 (as such term is defined in section 3(4) of the Na-
16 tional Security Act of 1947 (50 U.S.C. 3003(4))).

17 “(g) **USAGE.**—The national risk assessments and in-
18 tegrated national risk assessments required under sub-
19 section (f) shall be used to inform and guide allocation
20 of resources for cybersecurity and critical infrastructure
21 protection activities of the Department.

22 “(h) **INPUT AND SHARING.**—The Director shall, for
23 each national risk assessment and integrated national risk
24 assessment required under subsection (f)—

1 “(1) seek input from relevant Federal and non-
2 Federal entities involved in efforts to counter
3 threats;

4 “(2) ensure that written procedures are in place
5 to guide the development of such assessments, in-
6 cluding for input, review, and implementation pur-
7 poses, among relevant Federal entities;

8 “(3) share the classified versions of such assess-
9 ments with appropriate representatives from relevant
10 Federal and non-Federal entities with appropriate
11 security clearances and a need for such assessments;
12 and

13 “(4) to the maximum extent practicable, make
14 available the unclassified versions of such assess-
15 ments to relevant Federal and non-Federal entities
16 for cybersecurity and critical infrastructure protec-
17 tion.

18 “(i) COMPOSITION.—The Agency shall be composed
19 of the following divisions:

20 “(1) The Cybersecurity Division, headed by a
21 Principal Deputy Director.

22 “(2) The Infrastructure Protection Division,
23 headed by a Deputy Director.

24 “(3) The Emergency Communications Division
25 under title XVIII, headed by a Deputy Director.

1 “(4) The Federal Protective Service, headed by
2 a Deputy Director.

3 “(j) CONTRACTING AUTHORITY.—

4 “(1) DEFINITION.—In this subsection the term
5 ‘head of contracting activity’ means each official re-
6 sponsible for the creation, management, and over-
7 sight of a team of procurement professionals prop-
8 erly trained, certified, and warranted to accomplish
9 the acquisition of products and services on behalf of
10 the designated components, offices, and organiza-
11 tions of the Department, and as authorized, other
12 Federal Government entities.

13 “(2) APPLICATION.—All procurement and con-
14 tracting activities for the Agency shall be performed
15 in accordance with the Federal Acquisition Regula-
16 tion, the Department of Homeland Security Acquisi-
17 tion Policy, and other applicable laws, Federal regu-
18 lations, and policies.

19 “(3) DELEGATED AUTHORITY.—The Secretary,
20 acting through the Chief Procurement Officer of the
21 Department, may delegate procurement and con-
22 tracting authority to the Agency head of contracting
23 activity, as appropriate, after—

1 “(A) verifying that the head of contracting
2 activity has the training and experience to carry
3 out the authority to be delegated;

4 “(B) validating that Agency has identified
5 the personnel, systems, and resources to carry
6 out the authority to be delegated; and

7 “(C) providing Congress with a notification
8 of the delegation and attestations under para-
9 graphs (1) and (2).

10 “(4) PERFORMANCE REVIEW.—

11 “(A) IN GENERAL.—The Chief Procure-
12 ment Officer shall provide input on the periodic
13 performance review of the Agency’s head of
14 contracting activity.

15 “(B) RULE OF CONSTRUCTION.—None of
16 the authorities authorized in this subsection
17 shall prohibit the Chief Procurement Officer
18 from retaining contracting authority for the
19 Agency, as warranted.

20 “(5) COMPLIANCE.—The Agency shall comply
21 with Department policy prior to obligating funds
22 when using reimbursable work agreements or inter-
23 agency acquisitions with other Federal agencies or
24 Department components.

1 “(4) DEPARTMENT REVIEW.—Not later than
2 one year after any delegation pursuant to paragraph
3 (3), the Director shall report to Congress on the ex-
4 ercise of procurement and contracting authority by
5 the head of contracting activity of the Agency and
6 the status of Agency major acquisition programs,
7 cost, schedule, and performance.

8 “(k) STAFF.—

9 “(1) IN GENERAL.—The Secretary shall provide
10 the Agency with a staff of analysts having appro-
11 priate expertise and experience to assist the Agency
12 in discharging its responsibilities under this section.

13 “(2) PRIVATE SECTOR ANALYSTS.—Analysts
14 under this subsection may include analysts from the
15 private sector.

16 “(3) SECURITY CLEARANCES.—Analysts under
17 this subsection shall possess security clearances ap-
18 propriate for their work under this section.

19 “(l) DETAIL OF PERSONNEL.—

20 “(1) IN GENERAL.—In order to assist the
21 Agency in discharging its responsibilities under this
22 section, personnel of the Federal agencies referred to
23 in paragraph (2) may be detailed to the Agency for
24 the performance of analytic functions and related
25 duties.

1 “(2) AGENCIES SPECIFIED.—The Federal agen-
2 cies referred to in paragraph (1) are the following:

3 “(A) The Department of State.

4 “(B) The Central Intelligence Agency.

5 “(C) The Federal Bureau of Investigation.

6 “(D) The National Security Agency.

7 “(E) The National Geospatial-Intelligence
8 Agency.

9 “(F) The Defense Intelligence Agency.

10 “(G) Any other agency of the Federal Gov-
11 ernment that the President considers appro-
12 priate.

13 “(3) COOPERATIVE AGREEMENTS.—The Sec-
14 retary and the head of the agency concerned under
15 this subsection may enter into cooperative agree-
16 ments for the purpose of detailing personnel under
17 this subsection.

18 “(4) BASIS.—The detail of personnel under this
19 subsection may be on a reimbursable or non-reim-
20 bursable basis.

21 **“SEC. 2203. CYBERSECURITY DIVISION.**

22 “(a) ESTABLISHMENT.—

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

1 “(2) PRINCIPAL DEPUTY DIRECTOR.—The Cy-
2 bersecurity Division shall be headed by a Principal
3 Deputy Director of Cybersecurity (in this subtitle re-
4 ferred to as the ‘Principal Deputy Director’), who
5 shall—

6 “(A) be at the level of Assistant Secretary
7 within the Department; and

8 “(B) report to the Director.

9 “(3) REFERENCE.—Any reference to the Assist-
10 ant Secretary for Cybersecurity and Communica-
11 tions in any law, regulation, map, document, record,
12 or other paper of the United States shall be deemed
13 to be a reference to Principal Deputy Director of
14 Cybersecurity.

15 “(b) FUNCTIONS.—The Cybesecurity Division shall—

16 “(1) lead the cybersecurity efforts of the Agen-
17 cy;

18 “(2) carry out—

19 “(A) the Department’s activities related to
20 Federal information security; and

21 “(B) the functions of the national cyberse-
22 curity and communications integration center
23 under section 2209;

24 “(3) coordinate cybersecurity initiatives with
25 Federal and non-Federal entities for all activities re-

1 lating to stakeholder outreach, engagement, and
2 education, including engagement and coordination
3 activities for cybersecurity initiatives carried out by
4 the National Protection and Programs Directorate,
5 Office of Cybersecurity and Communications Stake-
6 holder Engagement and Cyber Infrastructure Resil-
7 ience division as of June 1, 2015;

8 “(4) provide coordination and support to non-
9 Federal entities to reduce cybersecurity risks, includ-
10 ing through voluntary partnerships;

11 “(4) conduct network and malicious code anal-
12 ysis for known and unknown cybersecurity threats;
13 and

14 “(5) in coordination with the Director, carry
15 out the consultation, coordination, and collaboration
16 required under subsection (d)(4) of section 2202.

17 “(c) ADDITIONAL FUNCTIONS.—In addition to the
18 responsibilities specified in subsection (b), the Principal
19 Deputy Director shall also—

20 “(1) under section 201, carry out paragraphs
21 (1), (3), (4), (5), (6), (8), (10), (11), (13), (14), and
22 (22) of subsection (d) of such section;

23 “(2) carry out comprehensive assessments of
24 the cybersecurity risks to critical infrastructure, in-
25 cluding the performance of risk assessments to de-

1 terminate the risks posed by particular types of ter-
2 rorist attacks within the United States (including an
3 assessment of the probability of success of such at-
4 tacks and the feasibility and potential efficacy of
5 various countermeasures to such attacks);

6 “(3) recommend cybersecurity measures nec-
7 essary to protect critical infrastructure in coordina-
8 tion with other Federal entities and in cooperation
9 with non-Federal entities; and

10 “(4) ensure that any material received pursuant
11 to this title is protected from unauthorized disclo-
12 sure and handled and used only for the performance
13 of official duties.

14 **“SEC. 2204. INFRASTRUCTURE PROTECTION DIVISION.**

15 “(a) ESTABLISHMENT.—

16 “(1) IN GENERAL.—There is established in the
17 Agency an Infrastructure Protection Division.

18 “(2) DEPUTY DIRECTOR.—The Infrastructure
19 Protection Division shall be headed by a Deputy Di-
20 rector of Infrastructure Protection (in this section
21 referred to as the ‘Deputy Director’), who shall re-
22 port to the Director.

23 “(3) REFERENCE.—Any reference to the Assist-
24 ant Secretary for Infrastructure Protection in any
25 law, regulation, map, document, record, or other

1 paper of the United States shall be deemed to be a
2 reference to Deputy Director of Infrastructure Pro-
3 tection.

4 “(b) FUNCTIONS.—The Infrastructure Protection Di-
5 vision shall—

6 “(1) lead the critical infrastructure protection
7 efforts of the Agency;

8 “(2) gather and manage critical infrastructure
9 information and ensure that such information is
10 available to the leadership of the Department and
11 critical infrastructure owners and operators;

12 “(3) lead the efforts of the Department to se-
13 cure the United States high-risk chemical facilities,
14 including the Chemical Facilities Anti-Terrorism
15 Standards established under title XXI;

16 “(4) provide coordination and support to non-
17 Federal entities to reduce risk to critical infrastruc-
18 ture from terrorist attack or natural disaster, includ-
19 ing through voluntary partnerships;

20 “(5) operate stakeholder engagement mecha-
21 nisms for appropriate critical infrastructure sectors,
22 except that such mechanisms may not duplicate any
23 engagement and coordination activities for cyberse-
24 curity initiatives carried out by the National Protec-
25 tion and Programs Directorate, Office of Cybersecu-

1 rity and Communications Stakeholder Engagement
2 and Cyber Infrastructure Resilience division as of
3 June 1, 2015;

4 “(6) administer the Coordinating Center estab-
5 lished under subsection (d);

6 “(7) in coordination with the Director, carry
7 out the consultation and collaboration required
8 under subsection (d)(4) of section 2202; and

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

11 “(c) ADDITIONAL FUNCTIONS.—In addition to the
12 responsibilities specified in subsection (b), the Deputy Di-
13 rector shall also—

14 “(1) under section 201, carry out paragraphs
15 (1), (3), (4), (5), (6), (8), (10), (11), (13), (14), and
16 (22) subsection (d) of such section;

17 “(2) carry out comprehensive assessments of
18 the vulnerabilities of critical infrastructure, including
19 the performance of risk assessments to determine
20 the risks posed by particular types of terrorist at-
21 tacks within the United States (including an assess-
22 ment of the probability of success of such attacks
23 and the feasibility and potential efficacy of various
24 countermeasures to such attacks);

1 “(3) recommend measures necessary to protect
2 critical infrastructure in coordination with other
3 Federal entities and in cooperation with non-Federal
4 entities; and

5 “(4) ensure that any material received pursuant
6 to this title is protected from unauthorized disclo-
7 sure and handled and used only for the performance
8 of official duties.

9 “(d) COORDINATING CENTER.—There shall be within
10 the Infrastructure Protection Division a National Infra-
11 structure Coordinating Center which shall be headed by
12 an Assistant Director and be co-located with the national
13 cybersecurity communications and integrated center estab-
14 lished under section 2209. The National Infrastructure
15 Coordinating Center shall—

16 “(1) collect, maintain, and share critical infra-
17 structure information;

18 “(2) evaluate critical infrastructure information
19 for accuracy, importance, and implications;

20 “(3) provide recommendations to non-Federal
21 entities and Department leadership;

22 “(4) advise the Secretary and the Director re-
23 garding actions required before and after a critical
24 infrastructure incident; and

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

3 (b) TREATMENT OF CERTAIN POSITIONS.—

4 (1) UNDER SECRETARY.—The individual serv-
5 ing as the Under Secretary appointed pursuant to
6 section 103(a)(1)(H) of the Homeland Security Act
7 of 2002 (6 U.S.C. 113(a)(1)) of the Department of
8 Homeland Security on the day before the date of the
9 enactment of this Act may continue to serve as the
10 Director of the Cybersecurity and Infrastructure
11 Protection Agency of the Department on and after
12 such date.

13 (2) DIRECTOR FOR EMERGENCY COMMUNICA-
14 TIONS.—The individual serving as the Director for
15 Emergency Communications of the Department of
16 Homeland Security on the day before the date of the
17 enactment of this Act may continue to serve as the
18 Deputy Director of Emergency Communications of
19 the Department on and after such date.

20 (3) ASSISTANT SECRETARY FOR CYBERSECU-
21 RITY AND COMMUNICATIONS.—The individual serv-
22 ing as the Assistant Secretary for Cybersecurity and
23 Communications on the day before the date of the
24 enactment of this Act may continue to serve as the
25 Principal Deputy Director of Cybersecurity.

1 (4) ASSISTANT SECRETARY FOR INFRASTRUC-
2 TURE PROTECTION.—The individual serving as the
3 Assistant Secretary for Infrastructure Protection on
4 the day before the date of the enactment of this Act
5 may continue to serve as the Deputy Director of In-
6 frastructure Protection.

7 (c) OPERATIONAL COORDINATION.—The Director of
8 the Cybersecurity and Infrastructure Protection Agency of
9 the Department of Homeland Security shall provide, in ac-
10 cordance with the deadlines specified in paragraphs (1)
11 and (2), to the Committee on Homeland Security of the
12 House and the Committee on Homeland Security and Gov-
13 ernmental Affairs of the Senate information on the fol-
14 lowing:

15 (1) Not later than 90 days after the date of the
16 enactment of this Act, the Agency’s mechanisms for
17 regular consultation and collaboration, including in-
18 formation on composition (including leadership
19 structure), authorities, frequency of meetings, and
20 visibility within the Agency.

21 (2) Not later than one year after the date of
22 the enactment of this Act, the activities of the Agen-
23 cy’s consultation and collaboration mechanisms and
24 how such mechanisms have impacted operational co-

1 ordination, situational awareness. and integration
2 across the Agency.

3 (d) CONFORMING AMENDMENTS.—The Homeland
4 Security Act of 2002 is amended—

5 (1) in section 103(a) (6 U.S.C. 113(a))—

6 (A) in paragraph (1), by amending sub-
7 paragraphs (H) and (I) to read as follows:

8 “(H) A Director of the Cybersecurity and In-
9 frastructure Protection Agency.

10 “(I) The Administrator of the Transportation
11 Security Administration.”; and

12 (B) by amending paragraph (2) to read as
13 follows:

14 “(2) OTHER ASSISTANT SECRETARIES AND OFFI-
15 CIALS.—

16 “(A) PRESIDENTIAL APPOINTMENTS.—The De-
17 partment shall have the following officers appointed
18 by the President:

19 “(i) The Principal Deputy Director of the
20 Cybersecurity Division under section 2203.

21 “(ii) The Assistant Secretary of the Office
22 of Public Affairs.

23 “(iii) The Assistant Secretary of the Office
24 of Legislative Affairs.

1 “(B) SECRETARIAL APPOINTMENTS.—The De-
2 partment shall have the following Assistant Secre-
3 taries appointed by the Secretary:

4 “(i) The Assistant Secretary for Inter-
5 national Affairs under section 602.

6 “(ii) The Assistant Secretary for Partner-
7 ship and Engagement under section 603.

8 “(C) LIMITATION ON CREATION OF POSI-
9 TIONS.—No Assistant Secretary position may be cre-
10 ated in addition to the positions provided for by this
11 section unless such position is authorized by a stat-
12 ute enacted after the date of the enactment of the
13 Cybersecurity and Infrastructure Protection Agency
14 Act of 2016.”;

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

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

18 (B) in the subtitle A heading, by striking
19 “**and Infrastructure Protection; Ac-**
20 **cess to Information**”;

21 (C) in section 201 (6 U.S.C. 121)—

22 (i) in the section heading, by striking
23 “**AND INFRASTRUCTURE PROTEC-**
24 **TION**”;

25 (ii) in subsection (a)—

1 (I) in the heading, by striking
2 “AND INFRASTRUCTURE PROTEC-
3 TION”; and

4 (II) by striking “and an Office of
5 Infrastructure Protection”;

6 (iii) in subsection (b)—

7 (I) in the heading, by striking
8 “AND ASSISTANT SECRETARY FOR IN-
9 FRASTRUCTURE PROTECTION”; and

10 (II) by striking paragraph (3);

11 (iv) in subsection (c)—

12 (I) by striking “and infrastruc-
13 ture protection”; and

14 (II) by striking “or the Assistant
15 Secretary for Infrastructure Protec-
16 tion, as appropriate”;

17 (v) in subsection (d)—

18 (I) in the heading, by striking
19 “AND INFRASTRUCTURE PROTEC-
20 TION”;

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

24 (III) by striking paragraphs (5)
25 and (6) and redesignating paragraphs

1 (7) through (25) as paragraphs (4)
2 through (23), respectively; and

3 (IV) by striking paragraph (23),
4 as so redesignated;

5 (vi) in subsection (e)(1), by striking
6 “and the Office of Infrastructure Protec-
7 tion”; and

8 (vii) in subsection (f)(1), by striking
9 “and the Office of Infrastructure Protec-
10 tion”;

11 (D) by redesignating sections 223 through
12 230 (6 U.S.C. 143–151) as sections 2205
13 through 2212, respectively, and inserting such
14 redesignated sections after section 2204, as
15 added by this Act;

16 (E) by redesignating section 210E (6
17 U.S.C. 124) as section 2213 and inserting such
18 redesignated section after section 2212;

19 (F) in subtitle B, by redesignating sections
20 211 through 215 (6 U.S.C. 101 note through
21 134) as sections 2214 through 2218, respec-
22 tively, and inserting such redesignated sections,
23 including the subtitle B designation (including
24 the enumerator and heading), after section
25 2213;

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

2 (A) in section 1801 (6 U.S.C. 571)—

3 (i) in the section heading, by striking

4 **“OFFICE OF EMERGENCY COMMU-**
5 **NICATIONS”** and inserting **“EMERGENCY**
6 **COMMUNICATIONS DIVISION”**;

7 (ii) in subsection (a)—

8 (I) by striking “Office of Emer-

9 gency Communications” and inserting

10 “Emergency Communications Divi-

11 sion”; and

12 (II) by adding at the end the fol-

13 lowing new sentence: “The Division

14 shall be located in the Cybersecurity

15 and Infrastructure Protection Agen-

16 cy.”; and

17 (iii) in subsection (b)—

18 (I) in the first sentence, by strik-

19 ing “Director for” and inserting

20 “Deputy Director of”; and

21 (II) in the second sentence, by

22 striking “Assistant Secretary for Cy-

23 bersecurity and Communications” and

24 inserting “Director of the Cybersecu-

1 rity and Infrastructure Protection
2 Agency”; and

3 (III) in subsection (e)—

4 (aa) in the matter preceding
5 paragraph (1), by striking “Di-
6 rector for” and inserting “Dep-
7 uty Director of”;

8 (bb) by redesignating para-
9 graphs (1) and (2) as paragraphs
10 (2) and (3), respectively; and

11 (cc) by inserting before
12 paragraph (2), as so redesign-
13 ated, the following new para-
14 graph:

15 “(1) with the Director of the Cybersecurity and
16 Infrastructure Protection Agency to carry out the
17 consultation and collaboration required under sub-
18 section (d)(4) of section 2202;”;

19 (B) in sections 1801 through 1805 (6
20 U.S.C. 575), by striking “Director for Emer-
21 gency Communications” each place it appears
22 and inserting “Deputy Director of Emergency
23 Communications”;

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

1 (i) by striking “Director for Emer-
2 gency Communications” each place it ap-
3 pears and inserting “Deputy Director of
4 Emergency Communications”; and

5 (ii) by striking “Office of Emergency
6 Communications” each place it appears
7 and inserting “Emergency Communica-
8 tions Division”;

9 (D) in section 1810 (6 U.S.C. 580)—

10 (i) by striking “Director” each place
11 it appears and inserting “Deputy Direc-
12 tor”;

13 (ii) by striking “Office of Emergency
14 Communications” each place it appears
15 and inserting “Emergency Communica-
16 tions Division”; and

17 (iii) in subsection (a)(1), by striking
18 “Director of the Office of Emergency Com-
19 munications (referred to in this section as
20 the ‘Director’)” and inserting “Deputy Di-
21 rector of the Emergency Communications
22 Division (referred to in this section as the
23 ‘Deputy Director’)”;

24 (4) in title XXI (6 U.S.C. 621 et seq.)—

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

1 (i) by redesignating paragraphs (4)
2 through (14) as paragraphs (5) through
3 (15), respectively;

4 (ii) by inserting after paragraph (3)
5 the following new paragraph:

6 “(4) the term ‘Director’ means the Director of
7 the Cybersecurity and Infrastructure Protection
8 Agency;”;

9 (iii) by further redesignating para-
10 graphs (11) through (15) (as redesignated
11 pursuant to clause (i)) as paragraphs (12)
12 through (16); and

13 (iv) by inserting after paragraph (10)
14 (as redesignated pursuant to clause (i)) the
15 following new paragraph:

16 “(11) the term ‘Secretary’ means the Secretary
17 acting through the Director;”;

18 (B) in paragraph (1) of section 2102(a) (6
19 U.S.C. 622(a)), by inserting at the end the fol-
20 lowing new sentence: “Such Programs shall be
21 located in the Cybersecurity and Infrastructure
22 Protection Agency.”; and

23 (C) in paragraph (2) of section 2104(c) (6
24 U.S.C. 624(c)), by striking “Under Secretary
25 responsible for overseeing critical infrastructure

1 protection, cybersecurity, and other related pro-
2 grams of the Department appointed under sec-
3 tion 103(a)(1)(H)” and inserting “Director of
4 the Cybersecurity and Infrastructure Protection
5 Agency”; and

6 (5) in title XXII, as added by this Act—

7 (A) in section 2205, as so redesignated, in
8 the matter preceding paragraph (1), by striking
9 “Under Secretary appointed under section
10 103(a)(1)(H)” and inserting “Director of the
11 Cybersecurity and Infrastructure Protection
12 Agency”;

13 (B) in section 2209, as so redesignated—

14 (i) by striking “Under Secretary ap-
15 pointed under section 103(a)(1)(H)” each
16 place it appears and inserting “Director of
17 the Cybersecurity and Infrastructure Pro-
18 tection Agency”;

19 (ii) in subsection (b), by adding at the
20 end the following new sentences: “The
21 Center shall be located in the Cybersecu-
22 rity and Infrastructure Protection Agency.
23 The head of the Center shall be an Assist-
24 ant Director of the Center, who shall re-

1 port to the Principal Deputy Director for
2 Cybersecurity.”; and

3 (iii) in subsection (c), by striking “Of-
4 fice of Emergency Communications” and
5 inserting “Emergency Communications Di-
6 vision”;

7 (C) in section 2210, as so redesignated—

8 (i) by striking “section 227” each
9 place it appears and inserting “section
10 2209”; and

11 (ii) in subsection (c), by striking
12 “Under Secretary appointed under section
13 103(a)(1)(H)” and inserting “Director of
14 the Cybersecurity and Infrastructure Pro-
15 tection Agency”;

16 (D) in section 2211, as so redesignated, by
17 striking “section 212(5)” and inserting “section
18 2215(5)”;

19 (E) in section 2212, as so redesignated, in
20 subsection (a)—

21 (i) in paragraph (3), by striking “sec-
22 tion 228” and inserting “section 2210”;
23 and

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

1 (e) CLERICAL AMENDMENT.—The table of contents
 2 in section 1(b) of the Homeland Security Act of 2002 is
 3 amended—

4 (1) by striking the item relating to section
 5 210E;

6 (2) by striking the items relating to section 211
 7 through section 215, including the subtitle B des-
 8 ignation (including the enumerator and heading);

9 (3) by striking the items relating to section 223
 10 through section 230; and

11 (4) by adding at the end the following new
 12 items:

“TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE
 PROTECTION AGENCY

“Subtitle A—Cybersecurity and Infrastructure Protection

- “Sec. 2201. Definitions.
- “Sec. 2202. Cybersecurity and Infrastructure Protection Agency.
- “Sec. 2203. Cybersecurity Division.
- “Sec. 2204. Infrastructure Protection 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. Clearances.
- “Sec. 2212. Federal intrusion detection and prevention system.
- “Sec. 2213. National Asset Database.

“Subtitle B—Critical Infrastructure Information

- “Sec. 2214. Short title.
- “Sec. 2215. Definitions.
- “Sec. 2216. Designation of critical infrastructure protection program.
- “Sec. 2217. Protection of voluntarily shared critical infrastructure information.
- “Sec. 2218. No private right of action.”.

1 **SEC. 3. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC**
2 **IDENTITY MANAGEMENT.**

3 (a) IN GENERAL.—Title VII of the Homeland Secu-
4 rity Act of 2002 (6 U.S.C. 341, et seq.) is amended by
5 adding at the end the following new section:

6 **“SEC. 708. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.**

7 “(a) ESTABLISHMENT.—The Office of Biometric
8 Identity Management is established within the Depart-
9 ment.

10 “(b) DIRECTOR.—

11 “(1) IN GENERAL.—The Office of Biometric
12 Identity Management shall be administered by the
13 Director of the Office of Biometric Identity Manage-
14 ment (in this section referred to as the ‘Director’)
15 who shall report to the Under Secretary for Manage-
16 ment, or to another official of the Department, as
17 the Under Secretary for Management may direct.

18 “(2) QUALIFICATIONS AND DUTIES.—The Di-
19 rector shall—

20 “(A) have significant professional manage-
21 ment experience, as well as experience in the
22 field of biometrics and identity management;

23 “(B) lead the Department’s biometric iden-
24 tity services to support anti-terrorism, counter-
25 terrorism, border security, credentialing, na-
26 tional security, and public safety, and enable

1 operational missions across the Department by
2 matching, storing, sharing, and analyzing bio-
3 metric data;

4 “(C) deliver biometric identity information
5 and analysis capabilities to—

6 “(i) the Department and its compo-
7 nents;

8 “(ii) appropriate Federal, State, local,
9 territorial, and tribal agencies;

10 “(iii) appropriate foreign govern-
11 ments; and

12 “(iv) appropriate private sector enti-
13 ties;

14 “(D) support the law enforcement, public
15 safety, national security, and homeland security
16 missions of other Federal, State, local, terri-
17 torial, and tribal agencies, as appropriate;

18 “(E) establish and manage the operation
19 and maintenance of the Department’s sole bio-
20 metric repository;

21 “(F) establish, manage, and operate Bio-
22 metric Support Centers to provide biometric
23 identification and verification analysis and serv-
24 ices to the Department, appropriate Federal,
25 State, local, territorial, and tribal agencies, ap-

1 appropriate foreign governments, and appropriate
2 private sector entities;

3 “(G) in collaboration with the Undersecre-
4 tary for Science and Technology, establish a
5 Department-wide research and development
6 program to support efforts in assessment, devel-
7 opment, and exploration of biometric advance-
8 ments and emerging technologies;

9 “(H) oversee Department-wide standards
10 for biometric conformity, and work to make
11 such standards Government-wide;

12 “(I) in coordination with the Department’s
13 Office of Policy, and in consultation with rel-
14 evant component offices and headquarters of-
15 fices, enter into data sharing agreements with
16 appropriate Federal agencies to support immi-
17 gration, law enforcement, national security, and
18 public safety missions;

19 “(J) maximize interoperability with other
20 Federal, State, local, and international biomet-
21 ric systems, as appropriate; and

22 “(K) carry out the duties and powers pre-
23 scribed by law or delegated by the Secretary.

24 “(c) DEPUTY DIRECTOR.—There shall be in the Of-
25 fice of Biometric Identity Management a Deputy Director,

1 who shall assist the Director in the management of the
2 Office.

3 “(d) CHIEF TECHNOLOGY OFFICER.—

4 “(1) IN GENERAL.—There shall be in the Office
5 of Biometric Identity Management a Chief Tech-
6 nology Officer.

7 “(2) DUTIES.—The Chief Technology Officer
8 shall—

9 “(A) ensure compliance with policies, proc-
10 esses, standards, guidelines, and procedures re-
11 lated to information technology systems man-
12 agement, enterprise architecture, and data
13 management;

14 “(B) provide engineering and enterprise
15 architecture guidance and direction to the Of-
16 fice of Biometric Identity Management; and

17 “(C) leverage emerging biometric tech-
18 nologies to recommend improvements to major
19 enterprise applications, identify tools to opti-
20 mize information technology systems perform-
21 ance, and develop and promote joint technology
22 solutions to improve services to enhance mission
23 effectiveness.

24 “(e) OTHER AUTHORITIES.—

1 “(1) IN GENERAL.—The Director may establish
2 such other offices within the Office of Biometric
3 Identity Management as the Director determines
4 necessary to carry out the missions, duties, func-
5 tions, and authorities of the Office.

6 “(2) NOTIFICATION.—If the Director exercises
7 the authority provided by paragraph (1), the Direc-
8 tor shall notify the Committee on Homeland Secu-
9 rity of the House of Representatives and the Com-
10 mittee on Homeland Security and Governmental Af-
11 fairs of the Senate not later than 30 days before ex-
12 ercising such authority.”.

13 (b) TRANSFER LIMITATION.—The Secretary of
14 Homeland Security may not transfer the location or re-
15 porting structure of the Office of Biometric Identity Man-
16 agement (established by section 708 of the Homeland Se-
17 curity Act of 2002, as added by subsection (a) of this sec-
18 tion) to any component of the Department of Homeland
19 Security.

20 (c) CLERICAL AMENDMENT.—The table of contents
21 in section 1(b) of the Homeland Security Act of 2002 is
22 amended by adding after the item relating to section 707
23 the following new item:

“Sec. 708. Office of Biometric Identity Management.”.

1 **SEC. 4. RULE OF CONSTRUCTION.**

2 Nothing in this Act may be construed to confer new
3 authorities to the Secretary of Homeland Security, includ-
4 ing programmatic and regulatory authorities, outside of
5 the authorities that existed on the day before the date of
6 the enactment of this Act.

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

8 No additional funds are authorized to be appro-
9 priated to carry out this Act or the amendments made
10 by this Act.

○