I

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity and Infrastructure Protection Agency Act of 2016''.

SEC. 2. CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY.

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

"TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY

"Subtitle A—Cybersecurity and Infrastructure Protection

"SEC. 2201. DEFINITIONS.

''In this subtitle—

''(1) CRITICAL INFRASTRUCTURE INCIDENT.—The term 'critical infrastructure incident' means an occurrence that actually or immediately jeopardizes, without lawful authority, the integrity, confidentially, or availability of critical infrastructure.

''(2) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given such term in section 2215.

''(3) CRITICAL INFRASTRUCTURE RISK.—The term 'critical infrastructure risk' means threats to and vulnerabilities of critical infrastructure and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such critical

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

''(4) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 2209.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given such term in paragraph (5) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(6) FEDERAL ENTITY.—The term 'Federal entity' has the meaning given such term in paragraph (8) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(7) NON-FEDERAL ENTITY.—The term 'non-Federal entity' has the meaning given such term in paragraph (14) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(8) SHARING.—The term 'sharing' has the meaning given such term in section 2209.

"SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY.

''(a) REDESIGNATION.—

''(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the 'Cybersecurity and Infrastructure Protection Agency' (in this subtitle referred to as the 'Agency').

''(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection Agency of the Department.

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

''(c) DIRECTOR.—

''(1) IN GENERAL.—The Agency shall be headed by a Director of National Cybersecurity (in this subtitle referred to as the 'Director').

''(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other re-

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

''(d) RESPONSIBILITIES.—The Director shall—

''(1) lead cybersecurity and critical infrastructure protection policy and operations for the Department;

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

''(3) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from threats;

''(4) maintain and utilize mechanisms, including a coordinating body for the regular and ongoing consultation and collaboration among the Agency's Divisions to further operation coordination, integrated situational awareness, and improved integration across the Agency;

''(5) develop, coordinate, and implement—

''(A) comprehensive strategic plans for cybersecurity and critical infrastructure protection; and

''(B) risk assessments for the Department, in accordance with subsection (f);

''(6) carry out emergency communications responsibilities, in accordance with title XVIII;

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

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

''(e) RISK ASSESSMENTS.—

''(1) NATIONAL RISK ASSESSMENTS.—The Director, in coordination with the heads of relevant components of the Department and other appropriate Federal entities, shall develop, coordinate, and update periodically (not less often than once every two years) a national risk assessment of—

''(A) cybersecurity risks; and

''(B) critical infrastructure risks.

''(2) INTEGRATED NATIONAL RISK ASSESSMENTS.—The Director shall develop, coordinate, and update periodically (not less often than once every

two years) an integrated national risk assessment that assesses all of the cybersecurity risks and critical infrastructure risks referred to in paragraph (1) and compares each such risk and incident against one another according to their relative risk, including cascading effects between each such risk.

''(3) INCLUSION IN ASSESSMENTS.—Each national risk assessment required under paragraph (1) and integrated national risk assessment required under paragraph (2) shall include—

''(A) a description of the data and methodology used for each such assessment; and

''(B) if applicable, actions or counter-measures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in each such assessment.

''(4) CLASSIFICATION.—The Director shall ensure that each national risk assessment required under paragraph (1) and integrated national risk assessment required under paragraph (2) has a classified and unclassified version.

''(5) PROVISION TO CONGRESS.—The Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Af-

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

''(f) METHODOLOGY.—In developing each national risk assessment required under subsection (f)(1) and integrated national risk assessment required under subsection (g)(2), the Director, in consultation with the heads of relevant Federal entities, shall—

''(1) assess the proposed methodology to be used for such assessments; and

''(2) consider the evolving threat to the United States as indicated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))).

''(g) USAGE.—The national risk assessments and integrated national risk assessments required under subsection (f) shall be used to inform and guide allocation of resources for cybersecurity and critical infrastructure protection activities of the Department.

''(h) INPUT AND SHARING.—The Director shall, for each national risk assessment and integrated national risk assessment required under subsection (f)—

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

''(2) ensure that written procedures are in place to guide the development of such assessments, including for input, review, and implementation purposes, among relevant Federal entities;

''(3) share the classified versions of such assessments with appropriate representatives from relevant Federal and non-Federal entities with appropriate security clearances and a need for such assessments; and

''(4) to the maximum extent practicable, make available the unclassified versions of such assessments to relevant Federal and non-Federal entities for cybersecurity and critical infrastructure protection.

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

''(1) The Cybersecurity Division, headed by a Principal Deputy Director.

''(2) The Infrastructure Protection Division, headed by a Deputy Director.

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

''(4) The Federal Protective Service, headed by a Deputy Director.

''(j) CONTRACTING AUTHORITY.—

''(1) DEFINITION.—In this subsection the term 'head of contracting activity' means each official responsible for the creation, management, and oversight of a team of procurement professionals properly trained, certified, and warranted to accomplish the acquisition of products and services on behalf of the designated components, offices, and organizations of the Department, and as authorized, other Federal Government entities.

''(2) APPLICATION.—All procurement and contracting activities for the Agency shall be performed in accordance with the Federal Acquisition Regulation, the Department of Homeland Security Acquisition Policy, and other applicable laws, Federal regulations, and policies.

''(3) DELEGATED AUTHORITY.—The Secretary, acting through the Chief Procurement Officer of the Department, may delegate procurement and contracting authority to the Agency head of contracting activity, as appropriate, after—

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

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

''(C) providing Congress with a notification of the delegation and attestations under paragraphs (1) and (2).

''(4) PERFORMANCE REVIEW.—

''(A) IN GENERAL.—The Chief Procurement Officer shall provide input on the periodic performance review of the Agency's head of contracting activity.

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

''(5) COMPLIANCE.—The Agency shall comply with Department policy prior to obligating funds when using reimbursable work agreements or interagency acquisitions with other Federal agencies or Department components.

''(4) DEPARTMENT REVIEW.—Not later than one year after any delegation pursuant to paragraph (3), the Director shall report to Congress on the exercise of procurement and contracting authority by the head of contracting activity of the Agency and the status of Agency major acquisition programs, cost, schedule, and performance.

''(k) STAFF.—

''(1) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging its responsibilities under this section.

''(2) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

''(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

''(l) DETAIL OF PERSONNEL.—

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

''(2) AGENCIES SPECIFIED.—The Federal agencies referred to in paragraph (1) are the following:

''(A) The Department of State.

''(B) The Central Intelligence Agency.

''(C) The Federal Bureau of Investigation.

''(D) The National Security Agency.

''(E) The National Geospatial-Intelligence Agency.

''(F) The Defense Intelligence Agency.

''(G) Any other agency of the Federal Government that the President considers appropriate.

''(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned under this subsection may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

''(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

''SEC. 2203. CYBERSECURITY DIVISION.

''(a) ESTABLISHMENT.—

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

''(2) PRINCIPAL DEPUTY DIRECTOR.—The Cybersecurity Division shall be headed by a Principal Deputy Director of Cybersecurity (in this subtitle referred to as the 'Principal Deputy Director'), who shall—

''(A) be at the level of Assistant Secretary within the Department; and

''(B) report to the Director.

''(3) REFERENCE.—Any reference to the Assistant Secretary for Cybersecurity and Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to Principal Deputy Director of Cybersecurity.

''(b) FUNCTIONS.—The Cybesecurity Division shall—

''(1) lead the cybersecurity efforts of the Agency;

''(2) carry out—

''(A) the Department's activities related to Federal information security; and

''(B) the functions of the national cybersecurity and communications integration center under section 2209;

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

lating to stakeholder outreach, engagement, and education, including engagement and coordination activities for cybersecurity initiatives carried out by the National Protection and Programs Directorate, Office of Cybersecurity and Communications Stakeholder Engagement and Cyber Infrastructure Resilience division as of June 1, 2015;

''(4) provide coordination and support to non-Federal entities to reduce cybersecurity risks, including through voluntary partnerships;

''(4) conduct network and malicious code analysis for known and unknown cybersecurity threats; and

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

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

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

''(2) carry out comprehensive assessments of the cybersecurity risks to critical infrastructure, including the performance of risk assessments to de-

termine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks);

''(3) recommend cybersecurity measures necessary to protect critical infrastructure in coordination with other Federal entities and in cooperation with non-Federal entities; and

''(4) ensure that any material received pursuant to this title is protected from unauthorized disclosure and handled and used only for the performance of official duties.

''SEC. 2204. INFRASTRUCTURE PROTECTION DIVISION.

''(a) ESTABLISHMENT.—

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

''(2) DEPUTY DIRECTOR.—The Infrastructure Protection Division shall be headed by a Deputy Director of Infrastructure Protection (in this section referred to as the 'Deputy Director'), who shall report to the Director.

''(3) REFERENCE.—Any reference to the Assistant Secretary for Infrastructure Protection in any law, regulation, map, document, record, or other

paper of the United States shall be deemed to be a reference to Deputy Director of Infrastructure Protection.

''(b) FUNCTIONS.—The Infrastructure Protection Division shall—

''(1) lead the critical infrastructure protection efforts of the Agency;

''(2) gather and manage critical infrastructure information and ensure that such information is available to the leadership of the Department and critical infrastructure owners and operators;

''(3) lead the efforts of the Department to secure the United States high-risk chemical facilities, including the Chemical Facilities Anti-Terrorism Standards established under title XXI;

''(4) provide coordination and support to non-Federal entities to reduce risk to critical infrastructure from terrorist attack or natural disaster, including through voluntary partnerships;

''(5) operate stakeholder engagement mechanisms for appropriate critical infrastructure sectors, except that such mechanisms may not duplicate any engagement and coordination activities for cybersecurity initiatives carried out by the National Protection and Programs Directorate, Office of Cybersecu-

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

''(6) administer the Coordinating Center established under subsection (d);

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

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

''(c) ADDITIONAL FUNCTIONS.—In addition to the responsibilities specified in subsection (b), the Deputy Director shall also—

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

''(2) carry out comprehensive assessments of the vulnerabilities of critical infrastructure, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks);

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

''(4) ensure that any material received pursuant to this title is protected from unauthorized disclosure and handled and used only for the performance of official duties.

''(d) COORDINATING CENTER.—There shall be within the Infrastructure Protection Division a National Infrastructure Coordinating Center which shall be headed by an Assistant Director and be co-located with the national cybersecurity communications and integrated center established under section 2209. The National Infrastructure Coordinating Center shall—

''(1) collect, maintain, and share critical infrastructure information;

''(2) evaluate critical infrastructure information for accuracy, importance, and implications;

''(3) provide recommendations to non-Federal entities and Department leadership;

''(4) advise the Secretary and the Director regarding actions required before and after a critical infrastructure incident; and

''(5) carry out such other duties and powers as prescribed by the Director.''.

(b) TREATMENT OF CERTAIN POSITIONS.—

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

(2) DIRECTOR FOR EMERGENCY COMMUNICATIONS.—The individual serving as the Director for Emergency Communications of the Department of Homeland Security on the day before the date of the enactment of this Act may continue to serve as the Deputy Director of Emergency Communications of the Department on and after such date.

(3) ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of the enactment of this Act may continue to serve as the Principal Deputy Director of Cybersecurity.

(4) ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of the enactment of this Act may continue to serve as the Deputy Director of Infrastructure Protection.

(c) OPERATIONAL COORDINATION.—The Director of the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security shall provide, in accordance with the deadlines specified in paragraphs (1) and (2), to the Committee on Homeland Security of the House and the Committee on Homeland Security and Governmental Affairs of the Senate information on the following:

(1) Not later than 90 days after the date of the enactment of this Act, the Agency's mechanisms for regular consultation and collaboration, including information on composition (including leadership structure), authorities, frequency of meetings, and visibility within the Agency.

(2) Not later than one year after the date of the enactment of this Act, the activities of the Agency's consultation and collaboration mechanisms and how such mechanisms have impacted operational co-

ordination, situational awareness. and integration across the Agency.

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

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

(A) in paragraph (1), by amending subparagraphs (H) and (I) to read as follows:

''(H) A Director of the Cybersecurity and Infrastructure Protection Agency.

''(I) The Administrator of the Transportation Security Administration.''; and

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

''(2) OTHER ASSISTANT SECRETARIES AND OFFICIALS.—

''(A) PRESIDENTIAL APPOINTMENTS.—The Department shall have the following officers appointed by the President:

''(i) The Principal Deputy Director of the Cybersecurity Division under section 2203.

''(ii) The Assistant Secretary of the Office of Public Affairs.

''(iii) The Assistant Secretary of the Office of Legislative Affairs.

''(B) SECRETARIAL APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the Secretary:

''(i) The Assistant Secretary for International Affairs under section 602.

''(ii) The Assistant Secretary for Partnership and Engagement under section 603.

''(C) LIMITATION ON CREATION OF POSITIONS.—No Assistant Secretary position may be created in addition to the positions provided for by this section unless such position is authorized by a statute enacted after the date of the enactment of the Cybersecurity and Infrastructure Protection Agency Act of 2016.'';

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

(A) in the title heading, by striking ''**AND INFRASTRUCTURE PROTECTION**'';

(B) in the subtitle A heading, by striking ''**and Infrastructure Protection; Access to Information**'';

(C) in section 201 (6 U.S.C. 121)—

(i) in the section heading, by striking ''**AND INFRASTRUCTURE PROTECTION**'';

(ii) in subsection (a)—

(I) in the heading, by striking ''AND INFRASTRUCTURE PROTECTION''; and

(II) by striking ''and an Office of Infrastructure Protection'';

(iii) in subsection (b)—

(I) in the heading, by striking ''AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION''; and

(II) by striking paragraph (3);

(iv) in subsection (c)—

(I) by striking ''and infrastructure protection''; and

(II) by striking ''or the Assistant Secretary for Infrastructure Protection, as appropriate'';

(v) in subsection (d)—

(I) in the heading, by striking ''AND INFRASTRUCTURE PROTECTION'';

(II) in the matter preceding paragraph (1), by striking ''and infrastructure protection'';

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

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

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

(vi) in subsection (e)(1), by striking ''and the Office of Infrastructure Protection''; and

(vii) in subsection (f)(1), by striking ''and the Office of Infrastructure Protection'';

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

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

(F) in subtitle B, by redesignating sections 211 through 215 (6 U.S.C. 101 note through 134) as sections 2214 through 2218, respectively, and inserting such redesignated sections, including the subtitle B designation (including the enumerator and heading), after section 2213;

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

(A) in section 1801 (6 U.S.C. 571)—

(i) in the section heading, by striking ''**OFFICE OF EMERGENCY COMMUNICATIONS**'' and inserting ''**EMERGENCY COMMUNICATIONS DIVISION**'';

(ii) in subsection (a)—

(I) by striking ''Office of Emergency Communications'' and inserting ''Emergency Communications Division''; and

(II) by adding at the end the following new sentence: ''The Division shall be located in the Cybersecurity and Infrastructure Protection Agency.''; and

(iii) in subsection (b)—

(I) in the first sentence, by striking ''Director for'' and inserting ''Deputy Director of''; and

(II) in the second sentence, by striking ''Assistant Secretary for Cybersecurity and Communications'' and inserting ''Director of the Cybersecu-

rity and Infrastructure Protection Agency''; and

(III) in subsection (e)—

(aa) in the matter preceding paragraph (1), by striking ''Director for'' and inserting ''Deputy Director of'';

(bb) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively; and

(cc) by inserting before paragraph (2), as so redesignated, the following new paragraph:

''(1) with the Director of the Cybersecurity and Infrastructure Protection Agency to carry out the consultation and collaboration required under subsection (d)(4) of section 2202;'';

(B) in sections 1801 through 1805 (6 U.S.C. 575), by striking ''Director for Emergency Communications'' each place it appears and inserting ''Deputy Director of Emergency Communications'';

(C) in section 1809 (6 U.S.C. 579)—

(i) by striking ''Director for Emergency Communications'' each place it appears and inserting ''Deputy Director of Emergency Communications''; and

(ii) by striking ''Office of Emergency Communications'' each place it appears and inserting ''Emergency Communications Division'';

(D) in section 1810 (6 U.S.C. 580)—

(i) by striking ''Director'' each place it appears and inserting ''Deputy Director'';

(ii) by striking ''Office of Emergency Communications'' each place it appears and inserting ''Emergency Communications Division''; and

(iii) in subsection (a)(1), by striking ''Director of the Office of Emergency Communications (referred to in this section as the 'Director')'' and inserting ''Deputy Director of the Emergency Communications Division (referred to in this section as the 'Deputy Director')'';

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

(A) in section 2101 (6 U.S.C. 621)—

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

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

''(4) the term 'Director' means the Director of the Cybersecurity and Infrastructure Protection Agency;'';

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

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

''(11) the term 'Secretary' means the Secretary acting through the Director;'';

(B) in paragraph (1) of section 2102(a) (6 U.S.C. 622(a)), by inserting at the end the following new sentence: ''Such Programs shall be located in the Cybersecurity and Infrastructure Protection Agency.''; and

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

protection, cybersecurity, and other related programs of the Department appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Protection Agency''; and

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

(A) in section 2205, as so redesignated, in the matter preceding paragraph (1), by striking ''Under Secretary appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Protection Agency'';

(B) in section 2209, as so redesignated—

(i) by striking ''Under Secretary appointed under section 103(a)(1)(H)'' each place it appears and inserting ''Director of the Cybersecurity and Infrastructure Protection Agency'';

(ii) in subsection (b), by adding at the end the following new sentences: ''The Center shall be located in the Cybersecurity and Infrastructure Protection Agency. The head of the Center shall be an Assistant Director of the Center, who shall re-

port to the Principal Deputy Director for Cybersecurity.''; and

(iii) in subsection (c), by striking ''Office of Emergency Communications'' and inserting ''Emergency Communications Division'';

(C) in section 2210, as so redesignated—

(i) by striking ''section 227'' each place it appears and inserting ''section 2209''; and

(ii) in subsection (c), by striking ''Under Secretary appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Protection Agency'';

(D) in section 2211, as so redesignated, by striking ''section 212(5)'' and inserting ''section 2215(5)''; and

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

(i) in paragraph (3), by striking ''section 228'' and inserting ''section 2210''; and

(ii) in paragraph (4), by striking ''section 227'' and inserting ''section 2209''.

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

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

(2) by striking the items relating to section 211 through section 215, including the subtitle B designation (including the enumerator and heading);

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

(4) by adding at the end the following new 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.".

SEC. 3. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

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

"SEC. 708. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

"(a) ESTABLISHMENT.—The Office of Biometric Identity Management is established within the Department.

"(b) DIRECTOR.—

"(1) IN GENERAL.—The Office of Biometric Identity Management shall be administered by the Director of the Office of Biometric Identity Management (in this section referred to as the 'Director') who shall report to the Under Secretary for Management, or to another official of the Department, as the Under Secretary for Management may direct.

"(2) QUALIFICATIONS AND DUTIES.—The Director shall—

"(A) have significant professional management experience, as well as experience in the field of biometrics and identity management;

"(B) lead the Department's biometric identity services to support anti-terrorism, counter-terrorism, border security, credentialing, national security, and public safety, and enable

operational missions across the Department by matching, storing, sharing, and analyzing biometric data;

"(C) deliver biometric identity information and analysis capabilities to—

"(i) the Department and its components;

"(ii) appropriate Federal, State, local, territorial, and tribal agencies;

"(iii) appropriate foreign governments; and

"(iv) appropriate private sector entities;

"(D) support the law enforcement, public safety, national security, and homeland security missions of other Federal, State, local, territorial, and tribal agencies, as appropriate;

"(E) establish and manage the operation and maintenance of the Department's sole biometric repository;

"(F) establish, manage, and operate Biometric Support Centers to provide biometric identification and verification analysis and services to the Department, appropriate Federal, State, local, territorial, and tribal agencies, ap-

propriate foreign governments, and appropriate private sector entities;

"(G) in collaboration with the Undersecretary for Science and Technology, establish a Department-wide research and development program to support efforts in assessment, development, and exploration of biometric advancements and emerging technologies;

"(H) oversee Department-wide standards for biometric conformity, and work to make such standards Government-wide;

"(I) in coordination with the Department's Office of Policy, and in consultation with relevant component offices and headquarters offices, enter into data sharing agreements with appropriate Federal agencies to support immigration, law enforcement, national security, and public safety missions;

"(J) maximize interoperability with other Federal, State, local, and international biometric systems, as appropriate; and

"(K) carry out the duties and powers prescribed by law or delegated by the Secretary.

"(c) DEPUTY DIRECTOR.—There shall be in the Office of Biometric Identity Management a Deputy Director,

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

''(d) CHIEF TECHNOLOGY OFFICER.—

''(1) IN GENERAL.—There shall be in the Office of Biometric Identity Management a Chief Technology Officer.

''(2) DUTIES.—The Chief Technology Officer shall—

''(A) ensure compliance with policies, processes, standards, guidelines, and procedures related to information technology systems management, enterprise architecture, and data management;

''(B) provide engineering and enterprise architecture guidance and direction to the Office of Biometric Identity Management; and

''(C) leverage emerging biometric technologies to recommend improvements to major enterprise applications, identify tools to optimize information technology systems performance, and develop and promote joint technology solutions to improve services to enhance mission effectiveness.

''(e) OTHER AUTHORITIES.—

''(1) IN GENERAL.—The Director may establish such other offices within the Office of Biometric Identity Management as the Director determines necessary to carry out the missions, duties, functions, and authorities of the Office.

''(2) NOTIFICATION.—If the Director exercises the authority provided by paragraph (1), the Director shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days before exercising such authority.''.

(b) TRANSFER LIMITATION.—The Secretary of Homeland Security may not transfer the location or reporting structure of the Office of Biometric Identity Management (established by section 708 of the Homeland Security Act of 2002, as added by subsection (a) of this section) to any component of the Department of Homeland Security.

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

''Sec. 708. Office of Biometric Identity Management.''.

SEC. 4. RULE OF CONSTRUCTION.

Nothing in this Act may be construed to confer new authorities to the Secretary of Homeland Security, including programmatic and regulatory authorities, outside of the authorities that existed on the day before the date of the enactment of this Act.

SEC. 5. PROHIBITION ON ADDITIONAL FUNDING.

No additional funds are authorized to be appropriated to carry out this Act or the amendments made by this Act.

○