Cybersecurity and Infrastructure Security Agency Act of 2018

[Public Law 115–278]

[This law has not been amended]

[Currency: This publication is a compilation of the text of Public Law 115-278. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at https://www.govinfo.gov/app/collection/comps/]

[Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).]

AN ACT 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.

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

SECTION 1. [6 U.S.C. 101 note] SHORT TITLE.

This Act may be cited as the "Cybersecurity and Infrastructure Security Agency Act of 2018".

SEC. 2. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

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

"TITLE TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

"SUBTITLE SUBTITLE A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

"SEC. SEC. 2201. [6 U.S.C. 651] DEFINITIONS

"In this subtitle:

"(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given the term in section 2222.

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

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

"(4) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

"(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

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

"(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

"(D) facilitating information sharing and operational coordination with threat response; and

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

"(5) SECTOR-SPECIFIC AGENCY.—The term 'Sector-Specific Agency' means a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

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

"SEC. SEC. 2202. [6 U.S.C. 652] CYBERSECURITY AND INFRASTRUCTURE SECURITY 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 Security 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 Security Agency of the Department.

"(b) DIRECTOR.—

"(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this subtitle referred to as the 'Director'), who shall report to the Secretary.

"(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of 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 Cybersecurity and Infrastructure Security of the Department.

"(c) RESPONSIBILITIES.—The Director shall—

"(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

"(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

"(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114-113));

"(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

"(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

"(6) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

"(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

"(8) develop, coordinate, and implement—

"(A) comprehensive strategic plans for the activities of the Agency; and

"(B) risk assessments by and for the Agency;

"(9) carry out emergency communications responsibilities, in accordance with title XVIII;

"(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; and

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

"(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

"(1) assist the Director in the management of the Agency; and

"(2) report to the Director.

"(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

"(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

"(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

"(i) identify and assess the nature and scope of terrorist threats to the homeland;

"(ii) detect and identify threats of terrorism against the United States; and

"(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

"(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, 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 those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

"(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

"(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

"(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

"(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in co-

operation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

"(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

"(H) To disseminate, as appropriate, information analyzed by the Department within the Department to other Federal Government agencies with responsibilities relating to homeland security and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

"(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

"(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

"(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

"(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

"(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

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

"(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

"(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

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

"(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

"(3) STAFF.—

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

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

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

"(4) DETAIL OF PERSONNEL.—

"(A) IN GENERAL.—In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

"(B) AGENCIES.—The Federal agencies described in this subparagraph are—

"(i) the Department of State;

"(ii) the Central Intelligence Agency;

"(iii) the Federal Bureau of Investigation;

"(iv) the National Security Agency;

"(v) the National Geospatial-Intelligence Agency;

"(vi) the Defense Intelligence Agency;

"(vii) Sector-Specific Agencies; and

"(viii) any other agency of the Federal Government that the President considers appropriate.

"(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

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

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

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

"(2) The Infrastructure Security Division, headed by an Assistant Director.

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

"(g) CO-LOCATION.—

"(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

"(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

"(h) PRIVACY.—

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

"(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

"(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

"(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the 'Privacy Act of 1974');

"(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

"(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

"(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of enactment of this title, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector-Specific Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114-94).

"SEC. SEC. 2203. [6 U.S.C. 653] CYBERSECURITY DIVISION

"(a) ESTABLISHMENT.—

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

"(2) ASSISTANT DIRECTOR.—The Cybersecurity Division shall be headed by an Assistant Director for Cybersecurity (in this section referred to as the 'Assistant Director'), who shall—

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

"(B) be appointed by the President without the advice and consent of the Senate; and

"(C) 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 the Assistant Director for Cybersecurity.

"(b) FUNCTIONS.—The Assistant Director shall—

"(1) direct the cybersecurity efforts of the Agency;

"(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114-113));

"(3) fully participate in the mechanisms required under section 2202(c)(7); and

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

"SEC. SEC. 2204. [6 U.S.C. 654] INFRASTRUCTURE SECURITY DIVISION

"(a) ESTABLISHMENT.—

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

"(2) ASSISTANT DIRECTOR.—The Infrastructure Security Division shall be headed by an Assistant Director for Infrastructure Security (in this section referred to as the 'Assistant Director'), who shall—

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

"(B) be appointed by the President without the advice and consent of the Senate; and

"(C) 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 the Assistant Director for Infrastructure Security.

"(b) FUNCTIONS.—The Assistant Director shall—

"(1) direct the critical infrastructure security efforts of the Agency;

"(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs;

"(3) fully participate in the mechanisms required under section 2202(c)(7); and

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

(b) TREATMENT OF CERTAIN POSITIONS.—

(1) [6 U.S.C. 652 note] 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)(H)) of the Department of Homeland Security on the day before the date of enactment of this Act may continue to serve as the Director of Cybersecurity and Infrastructure Security of the Department on and after such date.

(2) [6 U.S.C. 571 note] 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 enactment of this Act may continue to serve as the Assistant Director for Emergency Communications of the Department on and after such date.

(3) [6 U.S.C. 653 note] ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of enactment of this Act may continue to serve as the Assistant Director for Cybersecurity on and after such date.

(4) [6 U.S.C. 654 note] ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of enactment of this Act may continue to serve as the Assistant Director for Infrastructure Security on and after such date.

(c) [6 U.S.C. 571 note] REFERENCE.—Any reference to—

(1) the Office of Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Emergency Communications Division; and

(2) the Director for Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Emergency Communications.

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

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

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

(3) Not later than 90 days after the date of the enactment of this Act, information on the mechanisms of the Agency for regular and ongoing consultation and collaboration, as required pursuant to section 2202(c)(7) of the Homeland Security Act of 2002 (as added by subsection (a)).

(4) Not later than 1 year after the date of the enactment of this Act, information on the activities of the consultation and collaboration mechanisms of the Agency as required pursuant to section 2202(c)(7) of the Homeland Security Act of 2002, and how such mechanisms have impacted operational coordination, situational awareness, and integration across the Agency.

(5) Not later than 180 days after the date of enactment of this Act, information, which shall be made publicly available and updated as appropriate, on the mechanisms and structures of the Agency responsible for stakeholder outreach and engagement, as required under section 2202(c)(10) of the Homeland Security Act of 2002 (as added by subsection (a)).

(e) CYBER WORKFORCE.—Not later than 90 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, in coordination with the Director of the Office of Personnel Management, shall submit to Congress a report detailing how the Agency is meeting legislative requirements under the Cybersecurity Workforce Assessment Act (Public Law 113-246; 128 Stat. 2880) and the Homeland Security Cybersecurity Workforce Assessment Act (enacted as section 4 of the Border Patrol Agent Pay Reform Act of 2014; Public Law 113-277) to address cyber workforce needs.

(f) FACILITY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall report to Congress on the most efficient and effective methods of consolidating Agency facilities, personnel, and programs to most effectively carry out the Agency's mission.

(g) TECHNICAL AND CONFORMING AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

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

"(H) A Director of the Cybersecurity and Infrastructure Security Agency.";

(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";

(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 subsection heading, by striking "and Infrastructure Protection"; and

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

(iii) in subsection (b)—

(I) in the subsection 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 subsection heading, by striking "and Infrastructure Protection";

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

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

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

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

(VI) in paragraph (23)(B)(i), as so redesignated, by striking "section 319" and inserting "section 320";

(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) in section 202 (6 U.S.C. 122)—

(i) in subsection (c), in the matter preceding paragraph (1), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence"; and

(ii) in subsection (d)(2), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence";

(E) in section 204 (6 U.S.C. 124a)—

(i) in subsection (c)(1), in the matter preceding subparagraph (A), by striking "Assistant Secretary for Infrastructure Protection" and inserting "Director of the Cybersecurity and Infrastructure Security Agency"; and

(ii) in subsection (d)(1), in the matter preceding subparagraph (A), by striking "Assistant Secretary for Infrastructure Protection" and inserting "Director of the Cybersecurity and Infrastructure Security Agency";

(F) in section 210A(c)(2)(B) (6 U.S.C. 124h(c)(2)(B)), by striking "Office of Infrastructure Protection" and inserting "Cybersecurity and Infrastructure Security Agency";

(G) ⟦6 U.S.C. 664⟧ by redesignating section 210E (6 U.S.C. 124l) as section 2214 and transferring such section to appear after section 2213 (as redesignated by subparagraph (I));

(H) ⟦6 U.S.C. 671-674⟧ in subtitle B, by redesignating sections 211 through 215 (6 U.S.C. 101 note, and 131

through 134) as sections 2221 through 2225, respectively, and transferring such subtitle, including the enumerator and heading of subtitle B and such sections, to appear after section 2214 (as redesignated by subparagraph (G));

(I) ⟦6 U.S.C. 655-663⟧ by redesignating sections 223 through 230 (6 U.S.C. 143 through 151) as sections 2205 through 2213, respectively, and transferring such sections to appear after section 2204, as added by this Act;

(J) ⟦6 U.S.C. 124m⟧ by redesignating section 210F as section 210E; and

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

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

(A) in section 302 (6 U.S.C. 182)—

(i) by striking "biological,," each place that term appears and inserting "biological,"; and

(ii) in paragraph (3), by striking "Assistant Secretary for Infrastructure Protection" and inserting "Director of the Cybersecurity and Infrastructure Security Agency";

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

(C) in section 320(c)(1), as so redesignated, by striking "Section 214" and inserting "Section 2224";

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

(A) in section 508(d)(2)(D) (6 U.S.C. 318(d)(2)(D)), by striking "The Director of the Office of Emergency Communications of the Department of Homeland Security" and inserting "The Assistant Director for Emergency Communications";

(B) in section 514 (6 U.S.C. 321c)—

(i) by striking subsection (b); and

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

(C) in section 523 (6 U.S.C. 321l)—

(i) in subsection (a), in the matter preceding paragraph (1), by striking "Assistant Secretary for Infrastructure Protection" and inserting "Director of Cybersecurity and Infrastructure Security"; and

(ii) in subsection (c), by striking "Assistant Secretary for Infrastructure Protection" and inserting "Director of Cybersecurity and Infrastructure Security";

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

(A) in section 884(d)(4)(A)(ii) (6 U.S.C. 464(d)(4)(A)(ii)), by striking "Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department" and inserting "Director of Cybersecurity and Infrastructure Security"; and

(B) in section 899B(a) (6 U.S.C. 488a(a)), by adding at the end the following: "Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.";

(6) 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: "The Division shall be located in the Cybersecurity and Infrastructure Security Agency.";

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

"(b) ASSISTANT DIRECTOR.—The head of the Division shall be the Assistant Director for Emergency Communications. The Assistant Director shall report to the Director of Cybersecurity and Infrastructure Security. All decisions of the Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director of Cybersecurity and Infrastructure Security.";

(iv) in subsection (c)—

(I) in the matter preceding paragraph (1), by inserting "Assistant" before "Director";

(II) in paragraph (14), by striking "and" at the end;

(III) in paragraph (15), by striking the period at the end and inserting "; and"; and

(IV) by inserting after paragraph (15) the following:

"(16) fully participate in the mechanisms required under section 2202(c)(7).";

(v) in subsection (d), in the matter preceding paragraph (1), by inserting "Assistant" before "Director"; and

(vi) in subsection (e), in the matter preceding paragraph (1), by inserting "Assistant" before "Director";

(B) in sections 1802 through 1805 (6 U.S.C. 572 through 575), by striking "Director for Emergency Communications" each place that term appears and inserting "Assistant Director for Emergency Communications";

(C) in section 1809 (6 U.S.C. 579)—

(i) by striking "Director of Emergency Communications" each place that term appears and inserting "Assistant Director for Emergency Communications";

(ii) in subsection (b)—

(I) by striking "Director for Emergency Communications" and inserting "Assistant Director for Emergency Communications"; and

(II) by striking "Office of Emergency Communications" and inserting "Emergency Communications Division";

(iii) in subsection (e)(3), by striking "the Director" and inserting "the Assistant Director"; and

(iv) in subsection (m)(1)—

(I) by striking "The Director" and inserting "The Assistant Director";

(II) by striking "the Director determines" and inserting "the Assistant Director determines"; and

(III) by striking "Office of Emergency Communications" and inserting "Cybersecurity and Infrastructure Security Agency";

(D) in section 1810 (6 U.S.C. 580)—

(i) in subsection (a)(1), by striking "Director of the Office of Emergency Communications (referred to in this section as the 'Director')" and inserting "Assistant Director for Emergency Communications (referred to in this section as the 'Assistant Director')";

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

(iii) by striking "Director" each place that term appears and inserting "Assistant Director";

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

(A) in paragraph (4)(A)(iii)(II) of section 2001 (6 U.S.C. 601), by striking "section 210E(a)(2)" and inserting "section 2214(a)(2)";

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

(C) in section 2021 (6 U.S.C. 611)—

(i) by striking subsection (c); and

(ii) by redesignating subsection (d) as subsection (c);

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

(A) in section 2102(a)(1) (6 U.S.C. 622(a)(1)), by inserting ", which shall be located in the Cybersecurity and Infrastructure Security Agency" before the period at the end; and

(B) in section 2104(c)(2) (6 U.S.C. 624(c)(2)), 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 Cybersecurity and Infrastructure Security"; and

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

(A) in subtitle A—

(i) in section 2205, as so redesignated—

(I) in the matter preceding paragraph (1)—

(aa) by striking "section 201" and inserting "section 2202"; and

(bb) by striking "Under Secretary appointed under section 103(a)(1)(H)" and inserting "Director of Cybersecurity and Infrastructure Security"; and

(II) in paragraph (1)(B), by striking "and" at the end;

(ii) in section 2206, as so redesignated, by striking "Assistant Secretary for Infrastructure Protection" and

inserting "Director of Cybersecurity and Infrastructure Security";

(iii) in section 2209, as so redesignated—

(I) by striking "Under Secretary appointed under section 103(a)(1)(H)" each place that term appears and inserting "Director";

(II) in subsection (a)(4), by striking "section 212(5)" and inserting "section 2222(5)";

(III) in subsection (b), by adding at the end the following: "The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity."; and

(IV) in subsection (c)(11), by striking "Office of Emergency Communications" and inserting "Emergency Communications Division";

(iv) in section 2210, as so redesignated—

(I) by striking "section 227" each place that term appears and inserting "section 2209"; and

(II) in subsection (c)—

(aa) by striking "Under Secretary appointed under section 103(a)(1)(H)" and inserting "Director of Cybersecurity and Infrastructure Security"; and

(bb) by striking "section 212(5)" and inserting "section 2222(5)";

(v) in section 2211(b)(2)(A), as so redesignated, by striking "the section 227" and inserting "section 2209";

(vi) in section 2212, as so redesignated, by striking "section 212(5)" and inserting "section 2222(5)";

(vii) in section 2213(a), as so redesignated—

(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"; and

(viii) in section 2214, as so redesignated—

(I) by striking subsection (e); and

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

(B) in subtitle B—

(i) in section 2222(8), as so redesignated, by striking "section 227" and inserting "section 2209"; and

(ii) in section 2224(h), as so redesignated, by striking "section 213" and inserting "section 2223";

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

(1) CYBERSECURITY ACT OF 2015.—The Cybersecurity Act of 2015 (6 U.S.C. 1501 et seq.) is amended—

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

(i) by striking "section 227" and inserting "section 2209"; and

(ii) by striking ", as so redesignated by section 223(a)(3) of this division";

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

(i) by striking "section 227" and inserting "section 2209"; and

(ii) by striking ", as redesignated by section 223(a) of this division,";

(C) in section 208 (Public Law 114-113; 129 Stat. 2962), by striking "Under Secretary appointed under section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H))" and inserting "Director of Cybersecurity and Infrastructure Security of the Department";

(D) in section 222 (6 U.S.C. 1521)—

(i) in paragraph (2)—

(I) by striking "section 228" and inserting "section 2210"; and

(II) by striking ", as added by section 223(a)(4) of this division"; and

(ii) in paragraph (4)—

(I) by striking "section 227" and inserting "section 2209"; and

(II) by striking ", as so redesignated by section 223(a)(3) of this division";

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

(i) by striking "section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a)" each place that term appears and inserting "section 2213(b)(1) of the Homeland Security Act of 2002"; and

(ii) in paragraph (1)(B), by striking "section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a)" and inserting "section 2213(b)(2) of the Homeland Security Act of 2002";

(F) in section 226 (6 U.S.C. 1524)—

(i) in subsection (a)—

(I) in paragraph (1)—

(aa) by striking "section 230" and inserting "section 2213"; and

(bb) by striking ", as added by section 223(a)(6) of this division";

(II) in paragraph (4)—

(aa) by striking "section 228(b)(1)" and inserting "section 2210(b)(1)"; and

(bb) by striking ", as added by section 223(a)(4) of this division"; and

(III) in paragraph (5)—

(aa) by striking "section 230(b)" and inserting "section 2213(b)"; and

(bb) by striking ", as added by section 223(a)(6) of this division"; and

(ii) in subsection (c)(1)(A)(vi)—

(I) by striking "section 230(c)(5)" and inserting "section 2213(c)(5)"; and

(II) by striking ", as added by section 223(a)(6) of this division";

(G) in section 227 (6 U.S.C. 1525)—

(i) in subsection (a)—

(I) by striking "section 230" and inserting "section 2213"; and

(II) by striking ", as added by section 223(a)(6) of this division,"; and

(ii) in subsection (b)—

(I) by striking "section 230(d)(2)" and inserting "section 2213(d)(2)"; and

(II) by striking ", as added by section 223(a)(6) of this division,"; and

(H) in section 404 (6 U.S.C. 1532)—

(i) by striking "Director for Emergency Communications" each place that term appears and inserting "Assistant Director for Emergency Communications"; and

(ii) in subsection (a)—

(I) by striking "section 227" and inserting "section 2209"; and

(II) by striking ", as redesignated by section 223(a)(3) of this division,".

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

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

(A) in section 5314, by inserting after "Under Secretaries, Department of Homeland Security." the following:"Director, Cybersecurity and Infrastructure Security Agency."; and

(B) in section 5315, by inserting after "Assistant Secretaries, Department of Homeland Security." the following:"Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency. Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency.".

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

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

""TITLE II—INFORMATION ANALYSIS";"

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

"subtitle "Subtitle A—Information and Analysis; Access to Information";"

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

""Sec. 201. Information and analysis.";"

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

""Sec. 210E. Classified Information Advisory Officer.";"

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

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

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

"subtitle "Subtitle B—Information Security";"

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

"subtitle "Subtitle C—Office of Science and Technology";"

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

""Sec. 317. Promoting antiterrorism through international cooperation program.
""Sec. 318. Social media working group.
""Sec. 319. Transparency in research and development.
""Sec. 320. EMP and GMD mitigation research and development.";"

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

""Sec. 1801. Emergency Communications Division."; and"

(11) by adding at the end the following:

""TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

"subtitle "Subtitle A—Cybersecurity and Infrastructure Security

""Sec. 2201. Definitions.
""Sec. 2202. Cybersecurity and Infrastructure Security Agency.
""Sec. 2203. Cybersecurity Division.
""Sec. 2204. Infrastructure Security Division.
""Sec. 2205. Enhancement of Federal and non-Federal cybersecurity.
""Sec. 2206. Net guard.
""Sec. 2207. Cyber Security Enhancement Act of 2002.
""Sec. 2208. Cybersecurity recruitment and retention.
""Sec. 2209. National cybersecurity and communications integration center.
""Sec. 2210. Cybersecurity plans.
""Sec. 2211. Cybersecurity strategy.
""Sec. 2212. Clearances.
""Sec. 2213. Federal intrusion detection and prevention system.
""Sec. 2214. National Asset Database.

"subtitle "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."."

SEC. 3. [6 U.S.C. 452 note] TRANSFER OF OTHER ENTITIES.

(a) OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.—The Office of Biometric Identity Management of the Department of Homeland Security located in the National Protection and Programs Directorate of the Department of Homeland Security on the day before the date of enactment of this Act is hereby transferred to the Management Directorate of the Department.

(b) FEDERAL PROTECTIVE SERVICE.—

(1) IN GENERAL.—Not later than 90 days after the completion of the Government Accountability Office review of the organizational placement of the Federal Protective Service (au-

thorized under section 1315 of title 40, United States Code), the Secretary of Homeland Security shall determine the appropriate placement of the Service within the Department of Homeland Security and commence the transfer of the Service to such component, directorate, or other office of the Department that the Secretary so determines appropriate.

(2) EXCEPTION.—If the Secretary of Homeland Security determines pursuant to paragraph (1) that no component, directorate, or other office of the Department of Homeland Security is an appropriate placement for the Federal Protective Service, the Secretary shall—

(A) provide to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and the Office of Management and Budget a detailed explanation, in writing, of the reason for such determination that includes—

(i) information on how the Department considered the Government Accountability Office review described in such paragraph;

(ii) a list of the components, directorates, or other offices of the Department that were considered for such placement; and

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

(B) not later than 120 days after the completion of the Government Accountability Office review described in such paragraph, develop and submit to the committees specified in subparagraph (A) and the Office of Management and Budget a plan to coordinate with other appropriate Federal agencies, including the General Services Administration, to determine a more appropriate placement for the Service; and

(C) not later than 180 days after the completion of such Government Accountability Office review, submit to such committees and the Office of Management and Budget a recommendation regarding the appropriate placement of the Service within the executive branch of the Federal Government.

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

(a) DEFINITION.—In this section, the term "Department" means the Department of Homeland Security.

(b) REPORT.—Not later than 120 days after the date of enactment of this Act, the Secretary of Homeland Security, in coordination with the Director of the Office of Management and Budget and the Administrator of General Services, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform and the Committee on Homeland Security of the House of Representatives a report on the leadership role of the Department in cloud-

based cybersecurity deployments for civilian Federal departments and agencies, which shall include—

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

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

(A) criteria the Department will use to evaluate capabilities offered by the private sector; and

(B) how Federal government- and private sector-provided capabilities will be integrated to enable visibility and consistency of such capabilities across all cloud and on premise environments, as called for in the report described in paragraph (1); and

(3) information on how the Department will adapt the current capabilities of, and future enhancements to, the intrusion detection and prevention system of the Department and the Continuous Diagnostics and Mitigation Program of the Department to secure civilian Federal government networks in a cloud environment.

SEC. 5. [6 U.S.C. 651 note] RULE OF CONSTRUCTION.

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

(1) conferring new authorities to the Secretary of Homeland Security, including programmatic, regulatory, or enforcement authorities, outside of the authorities in existence on the day before the date of enactment of this Act;

(2) reducing or limiting the programmatic, regulatory, or enforcement authority vested in any other Federal agency by statute; or

(3) affecting in any manner the authority, existing on the day before the date of enactment of this Act, of any other Federal agency or component of the Department of Homeland Security.

SEC. 6. PROHIBITION ON ADDITIONAL FUNDING.

No additional funds are authorized to be appropriated to carry out this Act or the amendments made by this Act. This Act and the amendments made by this Act shall be carried out using amounts otherwise authorized.