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

IN THE HOUSE OF REPRESENTATIVES

Mr. McCaul introduced the following bill; which was referred to the Committee on ______________________

A BILL

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

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

2 SECTION 1. SHORT TITLE.

3 This Act may be cited as the “Cybersecurity and Infrastructure Security Agency Act of 2017”.

G:\VHLC\072017\072017.383.xml (66910611) July 20, 2017 (4:44 p.m.)
SEC. 2. CYBERSECURITY AND INFRASTRUCTURE SECURITY 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 SECURITY AGENCY

“Subtitle A—Cybersecurity and Infrastructure Security

“SEC. 2201. DEFINITIONS.

“In this subtitle:

“(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term ‘critical infrastructure information’ has the meaning given such term in section 2215.

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

“(3) CYBERSECURITY RISK.—The term ‘cybersecurity risk’ has the meaning given such term in section 2209.

“(4) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given such term in paragraph (5) of section 102 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)).

“(5) Federal entity.—The term ‘Federal entity’ has the meaning given such term in paragraph (8) of section 102 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)).

“(6) Non-Federal entity.—The term ‘non-Federal entity’ has the meaning given such term in paragraph (14) of section 102 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)).

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

“(8) National cybersecurity asset response activities.—The term ‘national cybersecurity asset response activities’ means—

“(A) furnishing 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.

“SEC. 2202. 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 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 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 and non-
Federal entities, including international entities, to
carry out the cybersecurity and critical infrastruc-
ture activities of the Agency, as appropriate;

“(3) carry out the Secretary’s responsibilities to
secure Federal information and information systems
consistent with law, including subchapter II of chap-
ter 35 of title 44, United States Code, and the Cy-
bersecurity 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;

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

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

“(7) maintain and utilize mechanisms for the
regular and ongoing consultation and collaboration
among the Agency’s Divisions to further operational
coordination, integrated situational awareness, and
improved integration across the Agency in accord-
ance with this Act;

“(8) develop, coordinate, and implement—

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

“(B) risk assessments;

“(9) carry out emergency communications re-

sponsibilities, in accordance with title XVIII;

“(10) carry out cybersecurity, infrastructure se-

curity, and emergency communications stakeholder
outreach and engagement; 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 Infra-
structure Security who shall—

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

“(2) report to the Director.

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

“(1) IN GENERAL.—The responsibilities of the
Secretary relating to cybersecurity and infrastruc-
ture 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 such 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 such 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 such attacks and the feasibility and
potential efficacy of various countermeasures to such attacks).

“(C) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis, or assessments are provided or produced by the Department) in order to identify priorities 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 such information from other Federal Government agencies.

“(E) To develop 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 prepared-
ness communications systems, and the physical
and technological assets that support such sys-
tems.

“(F) To recommend measures necessary to
protect the key resources and critical infra-
structure of the United States in coordination
with other Federal Government agencies and in
cooperation with State, local, tribal, and terri-
torial government agencies and authorities, the
private sector, and other entities.

“(G) To review, analyze, and make rec-
ommendations for improvements to the policies
and procedures governing the sharing of law en-
forcement information, and other information
relating to homeland security within the Fed-
eral Government and between Federal Govern-
ment agencies and State, local, tribal, and terri-
torial government agencies and authorities.

“(H) To disseminate, as appropriate, infor-
mation analyzed by the Department within the
Department, to other Federal Government
agencies with responsibilities relating to home-
land security, and to State, local, tribal, and
territorial government agencies and private sector entities with such responsibilities in order to assist in the deterrence, prevention, 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 ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

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

“(ii) treat information in such databases in a manner that complies with applicable Federal law on privacy.

“(N) 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 facili-
tate the identification and sharing of informa-
tion revealed in their ordinary duties and the
optimal utilization of information received from
the Department.

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

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

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

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

“(2) MODIFICATION.—The Secretary may mod-
ify the functions specified in sections 2203(b) and
2204(b) upon certifying to the Committee on Home-
land Security of the House of Representatives and
the Committee on Homeland Security and Government Affairs of the Senate 60 days prior to any such modification that such modification 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 its responsibilities 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 its responsibilities under this section, personnel of the Federal agencies referred to in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.
“(B) AGENCIES SPECIFIED.—The Federal agencies referred to in subparagraph (A) are the following:

“(i) The Department of State.
“(ii) The Central Intelligence Agency.
“(iii) The Federal Bureau of Investigation.
“(v) The National Geospatial-Intelligence Agency.
“(vi) The Defense Intelligence Agency.
“(vii) Any other agency of the Federal Government that the President considers appropriate.

“(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of an agency specified 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.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence. When establishing such locations, 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 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 Privacy Act systems of records of the Agency is handled in full compliance with fair information practices as specified in 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 the enactment of this title, of any other component of the Department or any other Federal department or agency.

“SEC. 2203. 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 subtitle referred to as the ‘Assistant 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 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 information and information systems for Federal entities 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 subsection (c)(7) of section 2202; and
“(4) carry out such other duties and powers as
prescribed by the Director.

“SEC. 2204. INFRASTRUCTURE SECURITY DIVISION.

“(a) ESTABLISHMENT.—

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

“(2) ASSISTANT DIRECTOR.—The Infrastruc-
ture Security Division shall be headed by an Assistant
Director of Infrastructure Security (in this sec-
tion referred to as the ‘Assistant 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 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 efforts, at the direction of the
Director, to secure the United States’ high-risk
chemicals and chemical facilities consistent with law, including the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate established under subtitle J of title VIII;

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

“(4) 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 Security 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
Assistant Director for 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 Assistant Director for Cybersecurity on and after such date.

(4) ASSISTANT SECRETARY FOR INFRASTRUCTURE SECURITY.—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 Assistant Director for Infrastructure Security on and after such date.

(e) 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 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 reference to the Assistant Director for Emergency Communications.

(d) OVERSIGHT.—The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to Congress, in accordance with the deadlines specified in paragraphs (1) and (2), information on the following:

(1) Not later than 90 days after the date of the enactment of this Act, information on the Agency’s mechanisms 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 this Act).

(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 coordination, situational awareness, and integration across the Agency.

(e) CYBER WORKFORCE.—Not later than 90 days after the date of the enactment of this subtitle, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to Congress a report detailing how the Agency is meeting legislative requirements under the Cybersecurity Work-
force Assessment Act (Public Law 113–246) 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 the 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) CONFORMING AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.—The Homeland Security Act of 2002 is amended—

(1) in title I, by amending subparagraph (H) of section 103(a)(1) (6 U.S.C. 113(a)(1)) 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 INFRASTRUCUTRE 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 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 (26) as paragraphs (5) through (24), respectively; 

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

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

(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 204 (6 U.S.C. 124a)— 

(i) in subsection (e)(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”;

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

(F) by transferring section 210E (6 U.S.C. 124) to appear after section 2212 (as redesignated by subparagraph (G) of this paragraph) and redesignating such section 210E as section 2214;

(G) in subtitle B, by redesignating sections 211 through 215 (6 U.S.C. 101 note through 134) as sections 2221 through 2225, respectively, and inserting such redesignated sections, including the enumerator and heading of subtitle B (containing such redesignated sections), after section 2213, as redesignated by subparagraph (E) of this paragraph; and
(H) by redesignating sections 223 through 230 (6 U.S.C. 143 through 151) as sections 2205 through 2213, respectively, and inserting such redesignated sections after section 2204, as added by this Act;

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

(4) in title V—

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

(i) striking subsection (b); and

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

(B) in section 523 (6 U.S.C. 321I)—

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

(ii) in subsection (c), by striking “Assistant Secretary for Infrastructure Protection” and inserting “Director of the Cyber-
security and Infrastructure Security Agen-

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

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

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

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

(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 COMMU-
NICATIONS” 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 Security Agency.”; and

(iii) in subsection (b)—

(I) in the first sentence, by inserting “Assistant” before “Director”; and

(II) in the second sentence, by striking “Assistant Secretary for Cybersecurity and Communications” and inserting “Director of the Cybersecurity and Infrastructure Security Agency”; 

(iv) in subsection (e)—

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

(II) in paragraph (14), by striking “and” at the end;
(III) by redesignating paragraph (15) as paragraph (16); and

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

“(15) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and”;

(v) in subsection (d), 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. 575), by striking “Director for Emergency Communications” each place it appears and inserting “Assistant Director for Emergency Communications”; 

(C) in section 1809 (6 U.S.C. 579)—

(i) by striking “Director for Emergency Communications” and inserting “Assistant Director for 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) 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 the Emergency Communications Division (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 it appears and inserting “Assistant Director”;

(7) 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; and

(ii) by inserting after paragraph (3) the following new paragraph:
“(4) the term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency;”;

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

(8) 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 Security Agency”; and

(B) in section 2206, as so redesignated, by striking “Assistant Secretary for Infrastructure
Protection” and inserting “Director of the Cybersecurity and Infrastructure Security Agency”;

(C) 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 Security Agency”;

(ii) in subsection (b), by adding at the end the following new sentences: “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

(iii) in subsection (c)(11), by striking “Office of Emergency Communications” and inserting “Emergency Communications Division”;

(D) 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 Secu-
rity Agency”;  

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

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

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

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

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

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

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

(1) in title II—
(A) in the item relating to the title heading, by striking “AND INFRASTRUCTURE PROTECTION”;

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

(C) in the item relating to section 201, by striking “AND INFRASTRUCTURE PROTECTION”;

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

(E) by striking the items relating to subtitle B of title II; and

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

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

“TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

Sec. 2201. Definitions.
Sec. 2202. Cybersecurity and Infrastructure Security Agency.
Sec. 2203. Cybersecurity Division.
Sec. 2204. Infrastructure Security Division.
Sec. 2206. Net guard.
Sec. 2208. Cybersecurity recruitment and retention.
Sec. 2209. National cybersecurity and communications integration center.
Sec. 2210. Cybersecurity plans.
Sec. 2211. Cybersecurity strategy.
Sec. 2212. Clearances.
Sec. 2213. Federal intrusion detection and prevention system.
Sec. 2214. National Asset Database.
Subtitle B—Critical Infrastructure Information

Sec. 2221. Short title.
Sec. 2222. Definitions.
Sec. 2223. Designation of critical infrastructure protection program.
Sec. 2224. Protection of voluntarily shared critical infrastructure information.
Sec. 2225. No private right of action.

SEC. 3. 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 the enactment of this Act is hereby transferred to the Management Directorate of the Department.

(b) Federal Protective Service.—The Secretary of Homeland Security is authorized to transfer the Federal Protective Service, as authorized under section 1315 of title 40, United States Code, to any component, directorate, or other office of the Department of Homeland Security that the Secretary determines appropriate.

SEC. 4. RULE OF CONSTRUCTION.

Nothing in 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 the 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 the enactment of this Act, of any other Federal agency or component of the Department of Homeland Security.

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. This Act and such amendments shall be carried out using amounts otherwise authorized.