6 U.S.C. § 652

Section 652 - Cybersecurity and Infrastructure Security Agency

(a) Redesignation

(1) In general

The National Protection and Programs Directorate of the Department shall, on and after November 16, 2018, be known as the "Cybersecurity and Infrastructure Security Agency" (in this part 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 part 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 113(a)(1)(H) of this title as in effect on the day before November 16, 2018, 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 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 chapter;

(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 subchapter XIII;

(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 122 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this subchapter, 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 cooperation 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 chapter 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 121(g) of this title.

(P) To carry out the functions of the national cybersecurity and communications integration center under section 659 of this title.

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

(2) Reallocation

The Secretary may reallocate within the Agency the functions specified in sections 653(b) and 654(b) of this title, 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 subchapter XIII, 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 (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 subchapter may be construed as affecting in any manner the authority, existing on the day before November 16, 2018, 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).

6 U.S.C. § 652

Pub. L. 107-296, title XXII, §2202, as added Pub. L. 115-278, §2(a), Nov. 16, 2018, 132 Stat. 4169.

REFERENCES IN TEXT*The Cybersecurity Act of 2015, referred to in subsec. (c)(3), is div. N of Pub. L. 114-113, 129 Stat. 2935. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.This chapter, referred to in subsecs. (c)(7) and (e)(1)(J), was in the original "this Act", meaning Pub. L. 107-296, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.*

UNDER SECRETARY RESPONSIBLE FOR OVERSEEING CRITICAL INFRASTRUCTURE PROTECTION, CYBERSECURITY AND RELATED PROGRAMS AUTHORIZED TO SERVE AS DIRECTOR OF CYBERSECURITY AND INFRASTRUCTURE SECURITY*Pub. L. 115-278, §2(b)(1), Nov. 16, 2018, 132 Stat. 4175, provided that: "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 [Nov. 16, 2018] may continue to serve as the Director of Cybersecurity and Infrastructure Security of the Department on and after such date."*