

“(iv) specific budget adjustments being requested to enhance United States security in a risk-based manner; and

“(v) the Federal departments and agencies responsible for the specific actions described in this subparagraph.

“(4) SUNSET.—The requirement to submit updated national strategies under this subsection shall terminate on the date that is seven years after the date of the enactment of this Act [Dec. 23, 2016].

“(c) DEVELOPMENT OF IMPLEMENTATION PLANS.—For each national strategy required under subsection (b), the President shall direct the heads of relevant Federal agencies to develop implementation plans for each such agency.

“(d) IMPLEMENTATION PLANS.—

“(1) IN GENERAL.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an implementation plan developed under subsection (c) with each national strategy required under subsection (b). Consistent with the protection of classified information, each such implementation plan shall be submitted in unclassified form, but may include a classified annex.

“(2) ANNUAL UPDATES.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an annual updated implementation plan during the ten-year period beginning on the date of the enactment of this Act [Dec. 23, 2016].

“(e) DEFINITION.—In this section, the term ‘appropriate congressional committees’ means—

“(1) in the House of Representatives—

“(A) the Committee on Homeland Security;

“(B) the Committee on Armed Services;

“(C) the Permanent Select Committee on Intelligence;

“(D) the Committee on the Judiciary;

“(E) the Committee on Foreign Affairs;

“(F) the Committee on Appropriations; and

“(2) in the Senate—

“(A) the Committee on Homeland Security and Governmental Affairs;

“(B) the Committee on Armed Services;

“(C) the Select Committee on Intelligence;

“(D) the Committee on the Judiciary;

“(E) the Committee on Foreign Relations; and

“(F) the Committee on Appropriations.

“(f) SPECIAL RULE FOR CERTAIN RECEIPT.—The definition under subsection (e) shall be treated as including the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate for purposes of receipt of those portions of—

“(1) the national strategy (including updates thereto), and

“(2) the implementation plan (including updates thereto),

required under this section that relate to maritime travel into and out of the United States.”

§ 124. Homeland Security Advisory System

(a) Requirement

The Secretary shall administer the Homeland Security Advisory System in accordance with this section to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal, State, local, and tribal government authorities and to the people of the United States, as appropriate. The Secretary shall exercise pri-

mary responsibility for providing such advisories or warnings.

(b) Required elements

In administering the Homeland Security Advisory System, the Secretary shall—

(1) establish criteria for the issuance and revocation of such advisories or warnings;

(2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of such advisories or warnings;

(3) provide, in each such advisory or warning, specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable to enable individuals, government entities, emergency response providers, and the private sector to act appropriately;

(4) whenever possible, limit the scope of each such advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and

(5) not, in issuing any advisory or warning, use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

(Pub. L. 107–296, title II, § 203, as added Pub. L. 110–53, title V, § 501(a)(1), Aug. 3, 2007, 121 Stat. 306.)

§ 124a. Homeland security information sharing

(a) Information sharing

Consistent with section 485 of this title, the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50) except for any internal security protocols or personnel information of such intelligence components, or other administrative processes that are administered by any chief security officer of the Department.

(b) Information sharing and knowledge management officers

For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3003(5) of title 50).

(c) State, local, and private-sector sources of information

(1) Establishment of business processes

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall—

(A) establish Department-wide procedures for the review and analysis of information

provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

(2) Feedback

The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of information provided by any entity of State, local, or tribal government or the private sector that provides such information to the Department.

(d) Training and evaluation of employees

(1) Training

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall provide to employees of the Department opportunities for training and education to develop an understanding of—

(A) the definitions of homeland security information and national intelligence (as defined in section 3003(5) of title 50); and

(B) how information available to such employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

(2) Evaluations

The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, as described in this subchapter, and participating in the information sharing environment established under section 485 of this title; and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

(Pub. L. 107–296, title II, §204, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 307; amended Pub. L. 115–278, §2(g)(2)(E), Nov. 16, 2018, 132 Stat. 4177.)

Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in subsec. (d)(2)(A), was in the original “this title”, meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Pro-

visions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c)(1), (d)(1). Pub. L. 115–278 substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Assistant Secretary for Infrastructure Protection” in introductory provisions.

Statutory Notes and Related Subsidiaries

RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERVICE

Pub. L. 110–53, title V, §502(b), Aug. 3, 2007, 121 Stat. 311, provided that:

“(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall receive from the United States Secret Service homeland security information, terrorism information, weapons of mass destruction information (as these terms are defined in Section [sic] 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)), or national intelligence, as defined in Section [sic] 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)) [now 50 U.S.C. 3003(5)], as well as suspect information obtained in criminal investigations. The United States Secret Service shall cooperate with the Under Secretary for Intelligence and Analysis with respect to activities under sections 204 and 205 of the Homeland Security Act of 2002 [6 U.S.C. 124a, 124b].

“(2) SAVINGS CLAUSE.—Nothing in this Act [see Tables for classification] shall interfere with the operation of Section [sic] 3056(g) of Title 18, United States Code, or with the authority of the Secretary of Homeland Security or the Director of the United States Secret Service regarding the budget of the United States Secret Service.”

§ 124b. Comprehensive information technology network architecture

(a) Establishment

The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 485 of this title, and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department.

(b) Comprehensive information technology network architecture defined

The term “comprehensive information technology network architecture” means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic management and information resources management goals of the Office of Intelligence and Analysis.

(Pub. L. 107–296, title II, §205, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 308.)