

advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

(Pub. L. 107–296, title II, §210E, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372.)

DEADLINES FOR IMPLEMENTATION AND NOTIFICATION OF CONGRESS

Pub. L. 110–53, title X, §1001(b), Aug. 3, 2007, 121 Stat. 374, provided that: “Not later than 180 days after the date of the enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall submit the first report required under section 210E(d) of the Homeland Security Act of 2002 [6 U.S.C. 124(d)], as added by subsection (a).”

§ 124m. Classified Information Advisory Officer

(a) Requirement to establish

The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

(b) Responsibilities

The responsibilities of the Classified Information Advisory Officer shall be as follows:

(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies) and private sector entities—

(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

(C) on the means by which such personnel may apply for security clearances.

(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

(c) Initial designation

Not later than 90 days after October 7, 2010, the Secretary shall—

(1) designate the initial Classified Information Advisory Officer; and

(2) submit to the Committee on Homeland Security and Governmental Affairs of the Sen-

ate and the Committee on Homeland Security of the House of Representatives a written notification of the designation.

(Pub. L. 107–296, title II, §210F, as added Pub. L. 111–258, §4(a), Oct. 7, 2010, 124 Stat. 2649.)

FINDINGS

Pub. L. 111–258, §2, Oct. 7, 2010, 124 Stat. 2648, provided that: “Congress finds the following:

“(1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the ‘9/11 Commission’) concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.

“(2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

“(3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.

“(4) Over-classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

“(5) Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification markings and the policies of the National Archives and Records Administration.”

§ 125. Annual report on intelligence activities of the Department of Homeland Security

(a) In general

For each fiscal year and along with the budget materials submitted in support of the budget of the Department of Homeland Security pursuant to section 1105(a) of title 31, the Under Secretary for Intelligence and Analysis of the Department shall submit to the congressional intelligence committees a report for such fiscal year on each intelligence activity of each intelligence component of the Department, as designated by the Under Secretary, that includes the following:

(1) The amount of funding requested for each such intelligence activity.

(2) The number of full-time employees funded to perform each such intelligence activity.

(3) The number of full-time contractor employees (or the equivalent of full-time in the case of part-time contractor employees) funded to perform or in support of each such intelligence activity.

(4) A determination as to whether each such intelligence activity is predominantly in support of national intelligence or departmental missions.

(5) The total number of analysts of the Intelligence Enterprise of the Department that perform—

(A) strategic analysis; or

(B) operational analysis.

(b) Feasibility and advisability report

Not later than 120 days after December 19, 2014, the Secretary of Homeland Security, acting

through the Under Secretary for Intelligence and Analysis, shall submit to the congressional intelligence committees a report that—

(1) examines the feasibility and advisability of including the budget request for all intelligence activities of each intelligence component of the Department that predominantly support departmental missions, as designated by the Under Secretary for Intelligence and Analysis, in the Homeland Security Intelligence Program; and

(2) includes a plan to enhance the coordination of department-wide intelligence activities to achieve greater efficiencies in the performance of the Department of Homeland Security intelligence functions.

(c) Intelligence component of the Department

In this section, the term “intelligence component of the Department” has the meaning given that term in section 101 of this title.

(Pub. L. 113–293, title III, §324, Dec. 19, 2014, 128 Stat. 4004.)

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

DEFINITIONS

“Congressional intelligence committees” means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives, see section 2 of Pub. L. 113–293, set out as a note under section 3003 of Title 50, War and National Defense.

PART B—CRITICAL INFRASTRUCTURE
INFORMATION

§ 131. Definitions

In this part:

(1) Agency

The term “agency” has the meaning given it in section 551 of title 5.

(2) Covered Federal agency

The term “covered Federal agency” means the Department of Homeland Security.

(3) Critical infrastructure information

The term “critical infrastructure information” means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment,

projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) Critical infrastructure protection program

The term “critical infrastructure protection program” means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) Information Sharing and Analysis Organization

The term “Information Sharing and Analysis Organization” means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a¹ interference, compromise, or a² incapacitation problem related to critical infrastructure or protected systems; and

(C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) Protected system

The term “protected system”—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) Voluntary

(A) In general

The term “voluntary”, in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency’s exercise of legal authority to compel access to or submission of such informa-

¹ So in original. Probably should be “an”.

² So in original. The word “a” probably should not appear.