(A) issue guidance for Department of Homeland Security employees authorized to access and contribute to the data framework pursuant to paragraph (1); and

(B) ensure that such guidance enforces a duty to share between offices and components of the Department when accessing or contributing to such framework for mission needs.

(3) Efficiency

The Secretary of Homeland Security shall promulgate data standards and instruct components of the Department of Homeland Security to make available information through the data framework required under this section in a machine-readable standard format, to the greatest extent practicable.

(c) Exclusion of information

The Secretary of Homeland Security may exclude information from the data framework required under this section if the Secretary determines inclusion of such information may—

(1) jeopardize the protection of sources, methods, or activities;

(2) compromise a criminal or national security investigation;

(3) be inconsistent with other Federal laws or regulations; or

(4) be duplicative or not serve an operational purpose if included in such framework.

(d) Safeguards

The Secretary of Homeland Security shall incorporate into the data framework required under this section systems capabilities for auditing and ensuring the security of information included in such framework. Such capabilities shall include the following:

(1) Mechanisms for identifying insider threats.

(2) Mechanisms for identifying security risks.

(3) Safeguards for privacy, civil rights, and civil liberties.

(e) Deadline for implementation

Not later than 2 years after December 19, 2018, the Secretary of Homeland Security shall ensure the data framework required under this section has the ability to include appropriate information in existence within the Department of Homeland Security to meet the critical mission operations of the Department of Homeland Security.

(f) Notice to Congress

(1) Status updates

The Secretary of Homeland Security shall submit to the appropriate congressional committees regular updates on the status of the data framework until the framework is fully operational.

(2) Operational notification

Not later than 60 days after the date on which the data framework required under this section is fully operational, the Secretary of Homeland Security shall provide notice to the appropriate congressional committees that the data framework is fully operational.

(3) Value added

The Secretary of Homeland Security shall annually brief Congress on component use of the data framework required under this section to support operations that disrupt terrorist activities and incidents in the homeland.

(g) Definitions

In this section:

(1) Appropriate congressional committee; homeland

The terms ''appropriate congressional committee'' and ''homeland'' have the meaning given those terms in section 101 of this title.

(2) Homeland security information

The term ''homeland security information'' has the meaning given such term in section 482 of this title.

(3) National intelligence

The term ''national intelligence'' has the meaning given such term in section 3003(5) of title 50.

(4) Terrorism information

The term ''terrorism information'' has the meaning given such term in section 485 of this title.

(Pub. L. 115–331, §2, Dec. 19, 2018, 132 Stat. 4484.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Department of Homeland Security Data Framework Act of 2018, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PART B—INFORMATION SECURITY

Editorial Notes

CODIFICATION

Subtitle C of title II of Pub. L. 107–296, which was classified to part C of this subchapter, was redesignated subtitle B of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

PRIOR PROVISIONS

A prior subtitle B of title II of Pub. L. 107–296, which was classified to this part, was redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to part B (§671 et seq.) of subchapter XVIII of this chapter.

§§ 131 to 134. Transferred

Editorial Notes

CODIFICATION

Section 131, Pub. L. 107–296, title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961, which related to definitions, was renumbered section 2222 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 671 of this title.

Section 132, Pub. L. 107–296, title II, §213, Nov. 25, 2002, 116 Stat. 2152, which related to designation of critical infrastructure protection program, was renumbered section 2223 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 672 of this title.

Section 133, Pub. L. 107–296, title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118

Stat. 814; Pub. L. 112–199, title I, § 111, Nov. 27, 2012, 126 Stat. 1472, which related to protection of voluntarily shared critical infrastructure information, was renumbered section 2224 of Pub. L. 107–296 by Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 673 of this title.

Section 134, Pub. L. 107–296, title II, § 215, Nov. 25, 2002, 116 Stat. 2155, which prohibited the construction of former part B as creating a private right of action for enforcement of any provision of this chapter, was renumbered section 2225 of Pub. L. 107–296 by Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 674 of this title.

§ 141. Procedures for sharing information

The Secretary shall establish procedures on the use of information shared under this subchapter that—

(1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of such information;

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(Pub. L. 107–296, title II, § 221, Nov. 25, 2002, 116 Stat. 2155.)

Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in text, 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 Provisions 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.

§ 142. Privacy officer

(a) Appointment and responsibilities

The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

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

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. 552a];

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974 [5 U.S.C. 552a], internal controls, and other matters.

(b) Authority to investigate

(1) In general

The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

(2) Enforcement of subpoenas

Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

(3) Effect of oaths

Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

(c) Supervision and coordination

(1) In general

The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.