each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

(g) Informing the public

Each privacy officer and civil liberties officer shall—

(1) make the reports of such officer, including reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and

(2) otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law.

(h) Savings clause

Nothing in this section shall be construed to limit or otherwise supplant any other authorities or responsibilities provided by law to privacy officers or civil liberties officers.

(Pub. L. 108–458, title I, §1062, Dec. 17, 2004, 118 Stat. 3688; Pub. L. 110–53, title VIII, §803(a), Aug. 3, 2007, 121 Stat. 360.)

AMENDMENTS

2007—Pub. L. 110–53 amended section generally. Prior to amendment, text of section read as follows: ''It is the sense of Congress that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer.''

§ 2000ee–2. Privacy and data protection policies and procedures

(a) Privacy Officer

Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including—

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

(2) assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program;

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

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

(5) conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected;

(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 section 552a of title 5, 11[1] internal controls, and other relevant matters;

(7) ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

(8) training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and

(9) ensuring compliance with the Departments[2] established privacy and data protection policies.

(b) Establishing privacy and data protection procedures and policies

(1)[3] In general

Within 12 months of December 8, 2004, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974 [5 U.S.C. 552a], and section 208 of the E-Government Act of 2002.

(c) Recording

Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report.

(d) Inspector General review

The Inspector General of each agency shall periodically conduct a review of the agency's implementation of this section and shall report the results of its review to the Committees on Appropriations of the House of Representatives and the Senate, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs. The report required by this review may be incorporated into a related report to Congress otherwise required by law including, but not limited to, section 3545 of title 44, the Fed-

[1] So in original.

[2] So in original. Probably should be ''Department's''.

[3] So in original. No par. (2) has been enacted.

eral Information Security Management Act of 2002. The Inspector General may contract with an independent, third party organization to conduct the review.

(e) Report

(1) In general

Upon completion of a review, the Inspector General of an agency shall submit to the head of that agency a detailed report on the review, including recommendations for improvements or enhancements to management of information in identifiable form, and the privacy and data protection procedures of the agency.

(2) Internet availability

Each agency shall make each independent third party review, and each report of the Inspector General relating to that review available to the public.

(f) Definition

In this section, the definition of ''identifiable form'' is consistent with Public Law 107–347, the E-Government Act of 2002, and means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

(Pub. L. 108–447, div. H, title V, § 522, Dec. 8, 2004, 118 Stat. 3268; Pub. L. 110–161, div. D, title VII, § 742(b), Dec. 26, 2007, 121 Stat. 2032.)

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsecs. (a)(3) and (b)(1), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

The Federal Information Security Management Act of 2002, referred to in subsec. (d), is the statutory short title for title III of Pub. L. 107–347, Dec. 17, 2002, 116 Stat. 2946, and for title X of Pub. L. 107–296, Nov. 25, 116 Stat. 2259. For complete classification of these Acts to the Code, see Short Title of 2002 Amendments note set out under section 101 of Title 44, Public Printing and Documents, Short Title note set out under section 101 of Title 6, Domestic Security, and Tables.

The E-Government Act of 2002, referred to in subsec. (f), is Pub. L. 107–347, Dec. 17, 2002, 116 Stat. 2899. Section 208 of the Act is set out as a note under section 3501 of Title 44, Public Printing and Documents. For complete classification of this Act to the Code, see Short Title of 2002 Amendments note set out under section 101 of Title 44 and Tables.

CODIFICATION

Section was formerly set out as a note under section 552a of Title 5, Government Organization and Employees.

AMENDMENTS

2007—Subsec. (d). Pub. L. 110–161 added subsec. (d) and struck out former subsec. (d) which related to independent, third-party reviews.

§ 2000ee–3. Federal agency data mining reporting

(a) Short title

This section may be cited as the ''Federal Agency Data Mining Reporting Act of 2007''.

(b) Definitions

In this section:

(1) Data mining

The term ''data mining'' means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

(2) Database

The term ''database'' does not include telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.

(c) Reports on data mining activities by Federal agencies

(1) Requirement for report

The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex described in subparagraph (C).[1]

(2) Content of report

Each report submitted under subparagraph (A)[2] shall include, for each activity to use or develop data mining, the following information:

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

(C) A thorough description of the data sources that are being or will be used.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with

[1] So in original. Probably should be ''paragraph (3)''.

[2] So in original. Probably should be ''paragraph (1)''.