the sense of Congress that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer.''

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019.

§ 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[4] of title 44, the Federal 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.)

[1] So in original.

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

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

[4] See References in Text note below.

Editorial Notes

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.

Section 3545 of title 44, referred to in subsec. (d), was repealed by Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073. Provisions similar to section 3545 of title 44 are now contained in section 3555 of title 44, as enacted by Pub. L. 113–283.

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.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019.

Executive Documents

EX. ORD. NO. 13719. ESTABLISHMENT OF THE FEDERAL PRIVACY COUNCIL

Ex. Ord. No. 13719, Feb. 9, 2016, 81 F.R. 7961, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. The mission of the United States Government is to serve its people. In order to accomplish its mission, the Government lawfully collects, maintains, and uses large amounts of information about people in a wide range of contexts. Protecting privacy in the collection and handling of this information is fundamental to the successful accomplishment of the Government's mission. The proper functioning of Government requires the public's trust, and to maintain that trust the Government must strive to uphold the highest standards for collecting, maintaining, and using personal data. Privacy has been at the heart of our democracy from its inception, and we need it now more than ever.

Executive departments and agencies (agencies) already take seriously their mission to protect privacy and have been working diligently to advance that mission through existing interagency mechanisms. Today's challenges, however, require that we find even more effective and innovative ways to improve the Government's efforts. Our efforts to meet these new challenges and preserve our core value of privacy, while delivering better and more effective Government services for the American people, demand leadership and enhanced coordination and collaboration among a diverse group of stakeholders and experts.

Therefore, it shall be the policy of the United States Government that agencies shall establish an interagency support structure that: builds on existing interagency efforts to protect privacy and provides expertise and assistance to agencies; expands the skill and career development opportunities of agency privacy professionals; improves the management of agency privacy programs by identifying and sharing lessons learned and best practices; and promotes collaboration between and among agency privacy professionals to reduce unnecessary duplication of efforts and to ensure the effective, efficient, and consistent implementation of privacy policy Government-wide.

SEC. 2. *Policy on Senior Agency Officials for Privacy*. Within 120 days of the date of this order, the Director of the Office of Management and Budget (Director) shall issue a revised policy on the role and designation of the Senior Agency Officials for Privacy. The policy shall provide guidance on the Senior Agency Official for Privacy's responsibilities at their agencies, required level of expertise, adequate level of resources, and other matters as determined by the Director. Agencies shall implement the requirements of the policy within a reasonable time frame as prescribed by the Director and consistent with applicable law.

SEC. 3. *Responsibilities of Agency Heads*. The head of each agency, consistent with guidance to be issued by the Director as required in section 2 of this order, shall designate or re-designate a Senior Agency Official for Privacy with the experience and skills necessary to manage an agency-wide privacy program. In addition, the head of each agency, to the extent permitted by law and consistent with ongoing activities, shall work with the Federal Privacy Council, established in section 4 of this order.

SEC. 4. *The Federal Privacy Council*.

(a) *Establishment*. There is hereby established the Federal Privacy Council (Privacy Council) as the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf. The establishment of the Privacy Council will help Senior Agency Officials for Privacy at agencies better coordinate and collaborate, educate the Federal workforce, and exchange best practices. The activities of the Privacy Council will reinforce the essential work that agency privacy officials undertake every day to protect privacy.

(b) *Membership*. The Chair of the Privacy Council shall be the Deputy Director for Management of the Office of Management and Budget. The Chair may designate a Vice Chair, establish working groups, and assign responsibilities for operations of the Privacy Council as he or she deems necessary. In addition to the Chair, the Privacy Council shall be composed of the Senior Agency Officials for Privacy at the following agencies:

(i) Department of State;
(ii) Department of the Treasury;
(iii) Department of Defense;
(iv) Department of Justice;
(v) Department of the Interior;
(vi) Department of Agriculture;
(vii) Department of Commerce;
(viii) Department of Labor;
(ix) Department of Health and Human Services;
(x) Department of Homeland Security;
(xi) Department of Housing and Urban Development;
(xii) Department of Transportation;
(xiii) Department of Energy;
(xiv) Department of Education;
(xv) Department of Veterans Affairs;
(xvi) Environmental Protection Agency;

(xvii) Office of the Director of National Intelligence;
(xviii) Small Business Administration;
(xix) National Aeronautics and Space Administration;
(xx) Agency for International Development;
(xxi) General Services Administration;
(xxii) National Science Foundation;
(xxiii) Office of Personnel Management; and
(xxiv) National Archives and Records Administration.

The Privacy Council may also include other officials from agencies and offices, as the Chair may designate, and the Chair may invite the participation of officials from such independent agencies as he or she deems appropriate.

(c) *Functions.* The Privacy Council shall:

(i) develop recommendations for the Office of Management and Budget on Federal Government privacy policies and requirements;

(ii) coordinate and share ideas, best practices, and approaches for protecting privacy and implementing appropriate privacy safeguards;

(iii) assess and recommend how best to address the hiring, training, and professional development needs of the Federal Government with respect to privacy matters; and

(iv) perform other privacy-related functions, consistent with law, as designated by the Chair.

(d) *Coordination.*

(i) The Chair and the Privacy Council shall coordinate with the Federal Chief Information Officers Council (CIO Council) to promote consistency and efficiency across the executive branch when addressing privacy and information security issues. In addition, the Chairs of the Privacy Council and the CIO Council shall coordinate to ensure that the work of the two councils is complementary and not duplicative.

(ii) The Chair and the Privacy Council should coordinate, as appropriate, with such other interagency councils and councils and offices within the Executive Office of the President, as appropriate, including the President's Management Council, the Chief Financial Officers Council, the President's Council on Integrity and Efficiency, the National Science and Technology Council, the National Economic Council, the Domestic Policy Council, the National Security Council staff, the Office of Science and Technology Policy, the Interagency Council on Statistical Policy, the Federal Acquisition Regulatory Council, and the Small Agency Council.

SEC. 5. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to a department, agency, or the head thereof; or

(ii) the functions of the Director relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) Independent agencies are encouraged to comply with the requirements of this order.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Ex. Ord. No. 13719 was originally published at 81 F.R. 7687 and was republished as set out above to correct an error appearing in the original publication.]

§ 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 and valuable to the stated goals and plans for the use or development of the data mining activity.

(E) An assessment of the impact or likely impact of the implementation of the data

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

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