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 mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to—

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

(3) Annex

(A) In general

A report under subparagraph (A)[2] shall include in an annex any necessary—

(i) classified information;

(ii) law enforcement sensitive information;

(iii) proprietary business information; or

(iv) trade secrets (as that term is defined in section 1839 of title 18).

(B) Availability

Any annex described in clause (i)—[3]

(i) shall be available, as appropriate, and consistent with the National Security Act of 1947 [50 U.S.C. 3001 et seq.], to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Financial Services of the House of Representatives; and

(ii) shall not be made available to the public.

(4) Time for report

Each report required under subparagraph (A)[2] shall be—

(A) submitted not later than 180 days after August 3, 2007; and

(B) updated not less frequently than annually thereafter, to include any activity to use or develop data mining engaged in after the date of the prior report submitted under subparagraph (A).[2]

(Pub. L. 110–53, title VIII, § 804, Aug. 3, 2007, 121 Stat. 362.)

REFERENCES IN TEXT

The National Security Act of 1947, referred to in subsec. (c)(3)(B)(i), is act July 26, 1947, ch. 343, 61 Stat. 495, which was formerly classified principally to chapter 15 (§ 401 et seq.) of Title 50, War and National Defense, prior to editorial reclassification in Title 50, and is now classified principally to chapter 44 (§ 3001 et seq.) of Title 50. For complete classification of this Act to the Code, see Tables.

CHAPTER 21F—PROHIBITING EMPLOYMENT DISCRIMINATION ON THE BASIS OF GENETIC INFORMATION

Sec.
2000ff. Definitions.

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

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

[3] So in original. Probably should be ''subparagraph (A)—''.