Department of Homeland Security
Management Directive System
MD Number: 0470.2
Issue date: 10/06/2005

PRIVACY ACT COMPLIANCE

I. Purpose

This Management Directive (MD) establishes the Department of Homeland Security (DHS) policy for Privacy Act Compliance.

II. Scope

This MD applies to all DHS Components, with the exception of the Office of Inspector General (OIG). The OIG, nevertheless, complies with all statutory privacy requirements.

III. Authorities

Numerous Public Laws and national policy govern this MD, such as:

A. The Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub .L. 93-579.

B. Section 222 of the Homeland Security Act of 2002, 6 U.S.C. § 142.

C. Section 208 of the E-Government Act of 2002, Pub. L. 107-347.

D. DHS Privacy Act Regulations, 68 FR 4056 (Jan. 27, 2003) as codified in 6 C.F.R. Chapter 1 and Part 5.

E. OMB Privacy Act Reference Materials available at: http://www.whitehouse.gov/omb/inforeg/infopoltech.html#pg.

IV. Definitions

A. ***Individual***: A citizen of the United States or an alien lawfully admitted for permanent residence.

B. ***Privacy Act Record***: Any item, collection, or grouping of information about an individual that is maintained by DHS in a system of records, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

C. ***Responsible Official***: The official having custody of the records requested, or a designated official, who makes initial determinations whether to grant or deny requests for notification, access to records, accounting of disclosures, and amendments of records.

D. ***System Manager***: The official identified in the system notice who is responsible for the operation and management of the system of records.

E. ***System of Records***: A group of any records under the control of DHS from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

F. ***Designated DHS Official***: Senior DHS officials as designated by the Secretary, Deputy Secretary, or Under Secretaries.

V. Responsibilities

System managers, program managers, and agency personnel (such as personnel specialists, finance officers, investigators, acquisition officials, attorneys/advisors, public affairs and disclosure officials) who have information contained in a system of records incident to the conduct of official business, shall be knowledgeable about the provisions and requirements of the Privacy Act and privacy provisions of the Homeland Security Act.

A. The ***Chief Privacy Officer*** shall:

1. Ensure that the use of technology sustains, and does not erode, privacy protections relating to the use, collection and disclosure of personal information.

2. Ensure the handling of personal information contained in Privacy Act systems of records is in full compliance with fair information practices in the Privacy Act of 1974.

3. Evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government.

4. Conduct a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected.

5. Prepare 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, internal controls, and other

matters.

6. Approve the notices and rules required to be published by the Privacy Act of 1974, as amended.

7. Act as the principal point of contact and the Department's representative for matters related to the Privacy Act.

8. Issue, and revise as needed, DHS regulations implementing the Privacy Act and review proposed changes to agency disclosure regulations.

9. In coordination with the Departmental Disclosure Officer, assign Privacy Act requests to appropriate responsible officials for action and follow up as necessary and notify a requester when all the information needed to process a request for records was not provided.

10. Collect, review, consolidate, and submit the data for the biennial Report to Congress on Computer Matching Programs for transmittal to OMB; and for the annual report to Congress on Department activities that affect privacy.

11. Coordinate, review, revise, and submit:

    a. The Privacy Act compilation of notices of DHS systems of records for publication in the *Federal Register*.

    b. Notices and reports on new or altered systems of records to the Office of Management and Budget (OMB), Congress, and the *Federal Register* on behalf of DHS.

    c. Notices on minor changes to systems of records to the *Federal Register* on behalf of DHS.

    d. Notices, reports, and proposed rules to OMB, Congress, and the *Federal Register* concerning exempt systems of records on behalf of DHS.

    e. Notices and reports for computer matches covered under the provisions of the Computer Matching and Privacy Protection Act of 1988 to OMB, Congress, and the *Federal Register* on behalf of DHS.

12. Report the results of reviews conducted by DHS Components as specified in OMB Circular A-130, Appendix I, paragraph 3.a., to the Director, OMB, including any corrective action taken.

13. Furnish policy, technical advice, and assistance to DHS Components on publication of notices of systems of records and the conduct of Privacy Impact Assessments.

14. Coordinate the implementation of the Privacy Act within DHS.

15. Ensure that all DHS Components:

a. Establish procedures necessary to carry out the provisions of this MD, OMB Circular A-130, Appendix I, and the Privacy Act.

b. Provide guidance for employees and contractors who are involved in designing, operating, or maintaining DHS Privacy Act systems of records.

c. Conduct Privacy Act training of employees and contractors who are involved in maintaining DHS Privacy Act systems of records or who have access to records contained in such systems.

16. Participate on government-wide task forces on computer technology concerned with establishing or affecting policies for collecting, compiling, using, maintaining, and safeguarding Federal Privacy Act systems of records.

B. The ***Under Secretaries and all DHS Designated Officials***, as it relates to their respective offices, shall:

1. Appoint an individual with day-to-day responsibility for implementing the privacy provisions of the Privacy Act, and any other applicable statutory privacy requirements.

2. Establish internal procedures to ensure the effectiveness of the DHS Privacy Act program and to safeguard individual privacy in the collection, compilation, maintenance, use, and dissemination of Federal records. The procedures shall be consistent with this MD and:

a. Section 222 of the Homeland Security Act of 2002.

b. The Privacy Act of 1974, as amended.

c. The Computer Matching and Privacy Protection Act of 1988.

d. The Federal Information Security Management Act.

e. OMB Circular A-130.

f. Applicable National Archives and Records Administration, Office of Personnel Management (OPM), and Office of Federal Register guidelines.

g. DHS privacy act regulations.

3. Submit the following, as required, to the Chief Privacy Officer for review and approval:

a. Accurate data for the Biennial Computer Matching Report to Congress and the Secretary's Annual Privacy Report to Congress.

b. Reports as required by OMB Circular A-130, or as required by the Chief Privacy Officer.

4. Submit the following, as required, to the Chief Privacy Officer for review and approval:

a. A notice and/or report for each new or altered system of records, along with the Privacy Impact Assessment.

b. A proposed and final rule, along with the Privacy Impact Assessment, for any determination to exempt a system of records.

c. A notice and report of the establishment or alteration of a matching program.

d. Any proposed rules or amendments to existing Privacy Act regulations, along with a Privacy Impact Assessment as appropriate, for review and concurrence prior to the review and concurrence procedures under MD-0490.

5. Establish an internal review of all office forms and data collection screens used to collect information, to include the Privacy Impact Assessment, about individuals to ensure that the forms and screens are in compliance with the Privacy Act and implementing regulations and guidelines.

C. The ***Under Secretary for Management*** shall:

1. Provide assistance as needed to the Chief Privacy Officer, especially regarding any proposed or anticipated change to computer installations, communications networks, or other electronic data collecting mechanisms, which may be potentially subject to the Privacy Act.

2. Assist DHS Components in the implementation of uniform and consistent policies and standards governing the acquisition, maintenance and use of computers or other electronic or telecommunications equipment in the collection, compilation, maintenance, use, or dissemination of Privacy Act records.

3. Provide security guidance to the components regarding the processing, storing, transferring, or receiving of information on individuals by computer, electronic or other telecommunications means or networks.

4. Participate in government-wide task forces on computer technology concerned with establishing or affecting policies for collecting, compiling, using, maintaining, and safeguarding Federal Privacy Act systems of records.

5. Provide the Chief Privacy Officer with proposed data collection screens, or other electronic data collecting mechanisms used to collect information about individuals, for Privacy Act compliance review, along with the Privacy Impact Assessment, prior to their use on the Intranet or Internet.

D. The ***Associate General Counsel for General Law*** shall serve as the primary legal counselor to the Chief Privacy Officer. The Associate General Counsel shall provide legal counsel to the Chief Privacy Office in the clearance of reports, notices of systems of records, proposed rules, and other related matters submitted by DHS to Congress, OMB and other parties. The Associate General Counsel for General Law shall handle all appeals of Privacy Act denials issued by the Departmental Disclosure Officer. The Associate General Counsel shall also provide legal counsel to the Chief Privacy Officer concerning Appeals of Privacy Act denials that are adjudicated by Component staff.

E. ***Systems Managers*** shall:

1. Ensure compliance with the Privacy Act and notify the Chief Privacy Officer when establishing, maintaining, revising, or deleting a system of records.

2. Establish administrative, technical, and physical controls for storing and safeguarding records. Subject to the internal operating procedures of the DHS Components, controls shall be consistent with DHS's security and recordkeeping regulations to ensure the protection of records systems from unauthorized access or disclosure, and from physical damage or destruction.

3. Establish and implement appropriate means for the accounting of disclosures made pursuant to the Privacy Act.

F. ***Responsible Officials*** shall:

1. Ensure that processing Privacy Act requests are in accordance with DHS disclosure regulations.

2. Determine whether to grant or deny requests for notification, access to records, accounting of disclosures, and amendments records.

3. Notify the requester of any determination(s) made pursuant to paragraph 5.F.(2).

4. Determine all costs for processing a request and determine whether duplication fees will be charged to the requester or waived.

5. Retrieve records retired to the Federal Records Center if they are needed to process a request.

G. ***Appeal Authorities***. The Associate General Counsel, General Law, is the DHS appeal authority from initial Privacy Act decisions made by the Departmental Disclosure Officer. He or she shall, upon receipt of a request for a review of a refusal by the Privacy Office to grant access, amend, or account for a record, either affirm or reverse the initial determination that denies access, amendment, or accounting of a record under the Privacy Act.

VI. Policy & Procedures

A. ***Policy***: All employees shall be made aware of, and comply with, the Privacy Act and ensure that information about individuals shall be collected, maintained, used, and disseminated in accordance with the Privacy Act and DHS regulations. Employees shall further be advised of the possible consequences for violations of the Privacy Act or DHS implementing authority.

B. ***Procedures***: DHS procedures for compliance with the Privacy Act are documented in the DHS Privacy Act Regulations, codified at 6 C.F.R. Part 5.

VII. Questions

Address any questions or concerns regarding this MD to the Chief Privacy Officer.