FY 2005 Report to Congress on Implementation of The E-Government Act of 2002 Promoting Information Privacy – Section 208

Federal agencies collect personal information about individuals for a variety of authorized purposes including to accurately determine program eligibility and to deliver efficient and effective services. Agencies must protect an individual's rights to information privacy by guarding against unauthorized disclosure or misuse of personal information. Accordingly, agencies take various measures to safeguard the personal information they collect.

To provide context, the following describes the Federal government's overall information privacy program including how agencies are implementing the E-Government Act's privacy provisions. This discussion also includes agency privacy program performance as reflected in their responses to OMB's new privacy reporting requirements.

Statutes and Policies Governing the Federal Government's Information Privacy Program

The Federal government's information privacy program relies primarily on five statutes which assign to OMB policy and oversight responsibilities:

- The Privacy Act of 1974 (5 U.S.C. § 552a) sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or identifier.
- The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a note) amended the Privacy Act to additionally provide a framework for the electronic comparison of personnel- and benefits-related information systems.
- The Paperwork Reduction Act of 1995 (44 U.S.C. § 101 note) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. §251 note) linked agency privacy activities to information technology and information resources management. Both assign to agency Chief Information Officers (CIO) the responsibility to ensure implementation of privacy programs within their respective agencies.
- Section 208 of the E-Government Act of 2002 included provisions requiring agencies to conduct privacy impact assessments[1] on new or substantially altered information technology systems and electronic information collections, and post web privacy policies at major entry points to their Internet sites.

[1] Privacy impact assessments analyze agency handling of personally identifiable information, describing for a specific system how the agency ensures compliance with law and policy and where protecting privacy demands modifications to the business process or information system.

As described further below, OMB's privacy policies are found in five guidance documents and referenced in many more, these include:

- Implementing the Privacy Act of 1974;
- Conducting matching programs under the Computer Matching and Privacy Protection Act of 1988;
- Completing privacy reports and other required publications;
- Implementing the privacy provisions of the E-Government Act of 2002; and
- Designating Senior Agency Officials for Privacy.

Implementing the Privacy Act of 1974. Following enactment of the Privacy Act of 1974, OMB issued comprehensive guidance for implementing the specific provisions of that Act (40 Fed. Reg. 28,949-28,978, July 9, 1975). This guidance defines statutory terms and explains notice and recordkeeping requirements as well as record subjects' rights of access and amendment.

Conducting matching programs under the Computer Matching and Privacy Protection Act of 1988. With the enactment of the Computer Matching amendments to the Privacy Act, OMB issued guidance on conducting matching programs (54 Fed. Reg. 25,819-25,829, June 19, 1989). This guidance defines statutory terms (i.e., coverage of the Act) and explains requirements and procedures for developing computer matching agreements.

Privacy reporting and publication requirements. In 1996, OMB issued Circular A-130, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals," amplifying on the guidance mentioned above, specifying content of and procedures for providing required public notices and describing agency obligations to report to OMB on privacy activities and compliance with the Act.[2]

Implementing the privacy provisions of the E-Government Act of 2002. In 2003, OMB issued guidance on implementing the E-Government Act's privacy requirements -- OMB Memorandum M-03-22 of September 26, 2003, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."[3]

Designating Senior Agency Officials for Privacy. Most recently, on February 11, 2005, OMB issued Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy," directing each executive Department and agency to identify a senior agency official for privacy to assume overall responsibility and accountability for ensuring agencies comply with privacy law and policy.[4] The memorandum directs these senior officials to coordinate development of all required agency reports, assume responsibility for agency activities relating to privacy, and address privacy policy issues at an agency-wide level. Specifically, the senior officials are responsible for:

---

[2] OMB Circular A-130, "Management of Federal Information Resources," can be found at: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

[3] OMB Memorandum M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," can be found at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[4] OMB Memorandum 05-08, "Designation of Senior Agency Officials for Privacy," can be found at: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf.

- overseeing, coordinating and facilitating agency compliance with privacy laws, regulations and policies, including maintaining appropriate documentation of compliance and ensuring remedial action for identified compliance weaknesses;
- ensuring the agency's employees and contractors receive appropriate training and education regarding information privacy laws, regulations, policies and procedures; and
- assuming a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy.

Agency Privacy Program Performance

OMB typically evaluates agency privacy compliance in three ways:

- Within the annual budget process, when agencies propose programs or investments in information technology systems;
- When agencies propose regulations or information collections under the Paperwork Reduction Act of 1995; and
- When agencies develop Privacy Act System of Records Notices and E-Government Act privacy impact assessments.

In 2005, OMB added two privacy oversight mechanisms. First, privacy was added to the quarterly President's Management Agenda Scorecard. Second, as part of agencies' annual reporting under the Federal Information Security Management Act, OMB asked agencies to report on how they are implementing the requirements of privacy laws and policy in the areas of privacy leadership and coordination, procedures and practices, and internal oversight.[5] In all areas, OMB works with agencies to address any reported underperformance.

Privacy and the President's Management Agenda

OMB added two criteria to the President's E-Government Management Agenda Scorecard to ensure agencies remain focused on their privacy responsibilities and integrate privacy into their E-Government activities. Agency progress in completing these criteria is evaluated each quarter. In order to maintain a successful evaluation of green on their agency scorecard, OMB measures whether an agency has:

- Conducted and publicly posted privacy impact assessments for at least ninety percent of applicable systems, and '
- Demonstrated they have developed and published Privacy Act Systems of Records Notices in at least ninety percent of required circumstances.[6]

[5] FISMA reporting instructions can be found at: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.html.
[6] A system of records is a group of any records under the control of any agency 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. The system of records notice documents the name and location of the system, the categories of individuals on whom records are maintained in the system, the categories of records maintained in the system, each routine use of the records contained in the system (including the categories of users and the purposes of such use), the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records, the title and business address of the agency official who is responsible for the system of records, the agency

Currently, 15 of 26 agencies evaluated each quarter by the President's Management Agenda Scorecard have conducted and publicly posted privacy impact assessments for ninety percent or more of applicable systems. Eighteen agencies have developed and published Privacy Act Systems of Records Notices in at least ninety percent of required circumstances.

Findings from Annual Reporting

1. Designating Senior Agency Official for Privacy

More than half of the 24 CFO Act agencies have designated their Chief Information Officer (CIO) as the Senior Agency Official for Privacy, while the remainder designated individuals at the Assistant Secretary, General Counsel, Deputy General Counsel, or component Director level. By contrast, approximately one-quarter to one-third of the small agencies designated CIOs to be their Senior Agency Official for Privacy, while the remainder were General Counsels, Executive Directors, Chief Financial Officers, or Administrators, as many of the micro-agencies (e.g., foundations, boards, commissions) have only a small executive staff with no specialized CIO position.

Of the 24 CFO Act agencies, 23 report their senior agency official for privacy: reviews compliance with agency information privacy activities; evaluates the privacy impact of legislative, regulatory and other policy proposals, as well as testimony and other formal communications; and assesses the impact of technology on the privacy of personal information.

2. Integrating Privacy Controls into Agency Operations

Agencies provided information about the degree to which they document their privacy program activities. Reports from the 24 CFO Act agencies indicate:

- twenty documented their review of compliance with information privacy laws, regulations and policies;
- seventeen provided planned, ongoing, or completed corrective actions addressing compliance deficiencies reported by the agency in a previous reporting period;
- twenty provided privacy training (both general and job specific) for employees and contractors, and conducted reviews of activities required by the Privacy Act and OMB policy;
- twenty-two established written policies and procedures for conducting privacy impact assessments;[7]

---

procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him, the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, including how he can contest its content, and the categories of sources of records in the system.

[7] Written policies and procedures for conducting privacy impact assessments help agencies determine whether a privacy impact assessment is needed, conduct an assessment in a consistent manner, evaluate changes in business processes or technology to properly identify when conducting an assessment may is necessary, ensure system owners, privacy experts, and information technology experts participate in conducting the assessment, and disseminate assessments to the public.

- fourteen performed privacy impact assessments as required for systems newly operational or substantially altered in the last year;
- twenty-one established a written process for determining compliance with agency website privacy policies;[8]
- twenty-two provided machine readable privacy policies (e.g., P3P-compliant or automatically readable using some other tool) on their websites and the remaining two plan to make their privacy policies machine readable by June 31, 2006;[9]
- twenty established a written process for determining continued compliance with persistent tracking policies;[10]
- twenty-four complied with the special authorization and notice requirements for persistent tracking;
- seven used persistent tracking and six have incorporated persistent tracking oversight into their privacy governance;
- eleven used technologies enabling continuous auditing of compliance with stated privacy policies and practices;
- nine submitted an annual report to Congress detailing their privacy activities, including activities under the Privacy Act and any violations; and
- ten provided to their Inspectors General (IG) materials helpful to program oversight including compilations of agency privacy and data protection policies and procedures, summaries of the agency's use of information in identifiable form, and verification of intent to comply with agency policies and procedures. OMB will follow up with agencies and their IGs to determine the extent to which IGs use these products for oversight purposes.

Cross-Government Privacy Coordination - OMB's Interagency Privacy Working Group

To promote a greater government-wide understanding of privacy responsibilities and assist agencies in fulfilling them, OMB leads an interagency working group comprising agency privacy specialists. The working group meets periodically to discuss issues of common interest such as data mining, use of commercial databases, and promising practices in implementing various statutory or policy requirements. To assist all agencies in implementing Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," the working group developed model system of records notices and privacy

[8] This written process helps agencies verify websites comply with the posted privacy policy and ensure corrective action is taken if any deficiencies are identified.

[9] The privacy policies inform users about what information the agency collects, and by what authority. P3P, or the "platform for privacy preferences," is an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. More information is at: http://www.w3.org/P3P/. Making privacy policies machine-readable ensures visitors to the site can ascertain quickly whether the agency's information handling practices conform to their individual preferences.

[10] Written processes ensure limited use of persistent tracking technology to those instances where a compelling need is identified and when authorized by agency head. It also helps ensure agencies review use of persistent tracking (when used) each year, continue to justify in writing and obtains approval to use the persistent tracking, and include language in the web privacy policy informing visitors when the persistent tracking technology is in use and for what purpose. OMB Memorandum M-00-13, "Privacy Policies and Data Collection on Federal Web Sites," located at: http://www.whitehouse.gov/omb/memoranda/m00-13.html provides privacy policies for agencies managing public websites.

impact assessments needed when developing systems using the new identification standard. The models were released by OMB in February, 2006