M99-05: Privacy and Personal Information in Federal Records

OMB Home

January 7, 1999

M-99-05

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew /s/

SUBJECT: Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"

This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14,1998 on "Privacy and Personal Information in Federal Records." In his Memorandum, the President directed Federal agencies to review their current information practices and ensure that they are being conducted in accordance with privacy law and policy. The President also directed OMB to issue instructions to the agencies on how to conduct this review.

Attached is a copy of the President's Memorandum, along with the instructions for conducting the review and for reporting to OMB on the results. Under the President's Memorandum, agencies are to complete their reviews and report to OMB by May 14, 1999.

Ensuring that the Federal government protects the privacy of personal information is a priority of this Administration. As stated by the President, privacy is a cherished American value. To preserve and promote this value, the United States created a statutory framework in 1974 governing how the Federal government collects, maintains, uses and disseminates information about certain individuals which is embodied in the Privacy Act, 5 U.S.C. § 552a, as amended. Earlier in this Administration in June 1995, the Information Infrastructure Task Force issued Principles for Providing and Using Personal Information as a statement of this Administration's policy on privacy.

The current review is an important part of the Administration's privacy agenda. We look forward to working with your agencies during this review.

Attachments

Attachment A -- Memorandum from the President

Attachment B -- Instructions for Complying with the President's Memorandum

Attachment C -- Governmentwide Systems of Records

M99-05

M99-05, Attachment A

M99-05, Attachment B

M99-05, Attachment C

Privacy Statement

M-99-05
Attachment B

INSTRUCTIONS FOR COMPLYING WITH THE PRESIDENT'S MEMORANDUM OF MAY 14, 1998, "Privacy and Personal Information in Federal Records"

A. WHAT IS THE PURPOSE OF THE REVIEW?

The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of systems of records containing personal information, to give individuals access to records about themselves in a system of records, and to manage those records in a way to ensure fairness to individuals in agency programs.

For the Privacy Act to work effectively, it is imperative that each agency properly maintain its systems of records and ensure that the public is adequately informed about the systems of records the agency maintains and the uses that are being made of the records in those systems. Therefore, agencies must periodically review their systems of records and the published notices that describe them to ensure that they are accurate and complete. OMB Circular A-130, "Management of Federal Information Resources," (61 Fed. Reg. 6428, Feb. 20, 1996) requires agencies to conduct periodic reviews, and this memorandum satisfies that requirement for calendar year FY 1999. Agencies should continue to conduct reviews in accordance with the schedule in Appendix I of the Circular.

In addition to directing agencies to ensure the accuracy and completeness of their systems of records, the President also directed agencies to review their data sharing practices with state, local and tribal governments.

B. WHAT ACTIONS MUST AGENCIES TAKE?

In order to carry out the President's directive, agencies will carry out six specific tasks. They should immediately designate a Senior Official for Privacy Policy if they have not already done so. They will review their systems of records, ensure that the notices published in the Federal Register describing those systems of records are up-to-date, and publish a notice for any system of records previously overlooked. They will also review information sharing practices with State, local, and tribal governments, and, finally, report to OMB the results of these reviews. More detailed instructions for each of these tasks follow.

1. Designate a Senior Official for Privacy Policy.

Each agency head should have already designated a senior official within the agency to assume primary responsibility for privacy policy, in accordance with the President's Memorandum. This individual will not necessarily be the same person who is responsible for implementation of the Privacy Act. For most

Cabinet agencies, the appropriate official would probably be a policy official at the Assistant Secretary level, or equivalent, who in a position within the agency to consider privacy policy issues on a national level.

Please notify OMB promptly of the name, title, address, phone number, and electronic mail address of the designated Senior Official for your agency.

2. Review and Improve the Management of Privacy Act Systems of Records.

Each agency shall conduct a thorough review of its systems of records, system of records notices, and routine uses in accordance with the criteria and guidance below. Because the President directed agencies to review systems of records, we have provided guidance on a subset of the Privacy Act's requirements that are particularly relevant to systems of records.

The goal is to focus agency resources on the most probable areas of out-of-date information, so that reviews will have the maximum impact in ensuring that system of records notices remain accurate and complete. An agency may rely on its ongoing reviews under Circular A-130 to help focus its review. An agency might decide to pay particular attention to identifying those systems of records that may have been altered by the application of new technology, changes in function, or changes in organizational structure that have occurred since the agency's last review of its systems of records. In addition, an agency may find the President's directive provides an opportunity to strengthen agency procedures to ensure reviews are timely conducted.

a. Information maintained about individuals must be relevant and necessary.

An important way for an agency to protect individual privacy is to limit the amount of information that the agency maintains about individuals. Therefore, each agency shall review its systems of records to ensure that they contain only that information about individuals that is "relevant and necessary" to accomplish an agency purpose.

The Privacy Act limits agencies to maintaining "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or Executive order of the President." 5 U.S.C. § 552a(e)(1). Information that was relevant and necessary when a system of records was first established may, over time, cease to be relevant or necessary. This may result, for example, from a change in agency function or reorganization, or from a change in how the agency operates a program.

If your agency determines that any information about individuals in a system of records is no longer relevant and necessary, or if your agency determines that the entire system of records itself is no longer relevant and necessary, then the agency should expunge the records (or system of records) in accordance with the procedures outlined in the Privacy Act notice(s) and the prescribed record retention schedule approved by the National Archives and Records Administration. The system notice should be accordingly revised (or rescinded).

b. Privacy Act records must be protected by appropriate safeguards.

For that information which agencies do maintain, agencies must ensure the information's security and confidentiality. Therefore, each agency shall review its systems of records to ensure that the safeguards in place are appropriate to the types of records and the level of security required.

The Privacy Act requires agencies to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained." 5 U.S.C. § 552a(e)(10). In addition, the Paperwork Reduction Act requires agencies to "implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency" and "identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency." 44 U.S.C. § 3506(g).

Over time, and given changes in how records are used and maintained, safeguards that may have been appropriate in the past may no longer be sufficient, or they may no longer be necessary. For example, safeguards that were appropriate for a system of records maintained in paper form may no longer be appropriate when the system of records has been converted to electronic form.

If your agency determines that changes to the safeguards should be made, then the agency should implement the changes and publish a system of records notice that reflects the updated safeguards. Note that the system of records notice should not state that access is limited to those who need the information in the course of their duties. Rather, the notice should explain how access is limited by describing the types of safeguards in place, such as locks, building access controls, passwords, network authentication, etc.

c. Routine uses must meet the "compatibility" standard.

Non-statutory disclosures created by administrative mechanisms should only be made when appropriate. Therefore, each agency shall review its "routine uses" to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected.

The Privacy Act authorizes agencies to disclose information about individuals under a "routine use." A routine use is defined as a disclosure of a record outside of the agency "for a purpose which is compatible with the purpose for which it was collected."5 U.S.C. § 552a(a)(7), (b)(3).

The Act requires agencies to include in their systems of records notices a description of the routine uses for which information in a system of records may be disclosed. 5 U.S.C. § 552a(e)(4)(D).

It may be the case that the circumstances which justified a routine-use disclosure have ceased to exist, or that the purpose for which the records are collected has changed over time so that the routine use no longer makes sense. Agencies should consult the Privacy Act Overview published by the Department of Justice each November (and available through the Government Printing Office) for judicial rulings which may affect the agency's routine uses. Such changes may well mean that the routine use is no longer justified or that the routine use is no longer compatible with the purpose for which the information is being collected. Agencies should review each routine use to ensure that each continues to be appropriate. In addition, agencies should review
the associated system of records notices to ensure that it accurately and completely describes the routine uses, including the categories of users and the purpose of such use.

If an agency determines that a routine use is no longer appropriate, the agency should discontinue the routine-use disclosures and delete the routine use from the system of records notice. If an agency determines that the system of records notice does not accurately and completely describe the routine uses, the agency should revise the notice accordingly.

d. Agencies must keep an accounting of disclosures and make it available.

In order to ensure fairness to individuals they must be able to determine who has seen their records and when they were seen. Therefore, each agency should review its procedures for accounting for disclosures to ensure they are working properly.

The Privacy Act requires agencies to "keep an accurate accounting" regarding "each disclosure of a record to any person or to another agency, "and to retain the accounting for at least five years or the life of the record, whichever is longer." 5 U.S.C. § 552a(c). As in the other contexts discussed above, "changes in technology, function, and organization" may result in accounting
procedures becoming outdated or may result in inadequate implementation of accounting procedures that remain appropriate.

An agency is relieved by the statute of accounting for disclosures made within the agency on a need-to-know basis or disclosure required by the Freedom of Information Act. 5 U.S.C. § 552a(c)(1). However, all other disclosures under 5 U.S.C. § 552a(b) must be accounted for, including those made under routine uses, and those made pursuant to requests from law
enforcement agencies (even though the latter may be exempt from disclosures to the subject individual). While an agency need not keep a running tabulation of every disclosure at the time it is made, the agency must be able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to requests in a timely fashion.

If an agency determines that changes to the accounting procedures should be made, then the agency should implement the changes promptly.

e. Systems of records should not be inappropriately combined.

Groups of records which have different purposes, routine uses, or security requirements, or which are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security. Therefore, agencies shall ensure that their systems of records do not inappropriately combine groups of records which should be segregated. This ensures, for example, that routine uses which are appropriate for certain groups of records do not also apply to other groups of records simply because they have been placed together in a common system of records.

Over time, changes in agency operations or functions may result in increased differences among the records that are contained within a common system of records. Groups of records that once were appropriately combined into a common system may have become sufficiently different that they should be divided into separate systems. Accordingly, during the course of the agency's review of its systems of records under **B.2.** of these instructions, and of its systems notices under **B.3.** of these instructions, an agency should identify instances where a system of records includes groups of records which -- because of their different purposes, routine uses, or security requirements -- should not be combined together into a common system of records, but instead should be maintained and managed as separate systems of records.

In addition, agency systems of records should not duplicate or be combined with those systems which have been designated as "government wide systems of records." A government wide system of records is one for which one agency has regulatory authority over records in the custody of many different agencies. Usually these are federal personnel or administrative records. Such government-wide systems ensure that privacy practices with respect to those records are carried out in accordance with the responsible agency's regulations uniformly across the federal government. For example, a civilian agency subject to the personnel rules of the Office of Personnel Management should manage its official personnel folders in accordance with the government wide notice published by OPM for those records, OPM/GOVT-1. The custodial agency need not, and should not, publish a system of records which covers the same records. A list of government-wide systems of records may be found at Attachment C, along with the name of someone who can answer specific questions about those systems of records.

3. Ensure notices describing systems of records are up-to-date, accurate and complete.

In order to exercise their rights, individuals must have access to an up-to-date statement of what types of information are maintained and for what reasons. Therefore, each agency shall conduct a review of its systems of records notices to ensure that they are up-to-date, to conform with any necessary changes identified during the review under section **B.2.** of these instructions.

The Privacy Act requires agencies to publish, upon the establishment of a system of records, a notice that describes the system. 5 U.S.C. § 552a(e)(4). The core purpose of a system of records notice is to inform the public what types of records the agency maintains, who the records are about, and what uses are made of them. As the President noted in his Memorandum, however, "changes in technology, function, and organization" may have the effect of making system of records notices "out of date."

A systems of records notice should accurately and completely describe each category in the notice to comply with the requirements of 5 U.S.C. § 552a(e)(4) and the Federal Register Document Drafting Handbook. (The Handbook can be found at the web page of National Archives and Records Administration (NARA), at http://www.nara.gov/fedreg/draftres.html
or by contacting the Office of the Federal Register.) The goal is to provide a notice helpful to someone who might be a subject of the records. The reviewer should ask, "If this system of records contained information about my friends or relatives, would this notice allow them to understand what type of records are kept, who uses them, and why?"

Agencies should take note that the descriptive categories for systems of records notices have changed over time. For example, the Drafting Handbook now requires that each system of records include a Purpose statement. This statement should briefly explain the program purpose for which the records are collected and which the system of records supports.

While a notice-by-notice review may be appropriate, an agency may also decide to concentrate its review by focusing on those notices that are more likely to contain outdated information. An agency using this targeted approach, for example, could begin its review by identifying changes in technology, function, and organization -- that is, changes in how the agency operates -- that
would have the potential to make a system of records notice out-of-date. Based on this analysis, the agency would then identify those systems of records that would most likely have been affected by these changes in agency operations. Under this approach, an agency should focus its review on those notices that apply to systems of records that have been automated; that are operated by an office (or for a program) that has been assigned increased (or decreased) responsibilities; or that have been involved in an agency reorganization. This is not meant to be an exhaustive list; an agency should seek to identify other ways in which changing agency operations may have affected the accuracy and completeness of its systems of records notices.

4. Identify any Unpublished Systems of Records.

In passing the Privacy Act, the Congress made a strong policy statement that in order to ensure fairness, there shall be no record keeping systems the very existence of which is secret. Therefore, each agency shall review its operations to identify any de facto systems of records for which no system of records notice has been published.

If the agency identifies any such unpublished systems of records, then the agency should publish a system of records notice for the system promptly. Agencies shall implement appropriate measures (e.g., training) to ensure that system of records are not inadvertently established, but instead are established in accordance with the notice and other requirements of the Privacy Act.

5. Review Information Sharing Practices with State, Local and Tribal Governments.

In accordance with the President's May 14, 1998, directive and the Vice President's announcement on July 31 that the Administration intends to open a dialogue with the States about information sharing, each agency shall review their practices of sharing personal information with State, local and tribal governments. This review should include a review of the agency's systems of records, computer matching programs, and routine uses which provide for intergovernmental collection or disclosure of information. Agencies should not survey the States to collect information, but should use internal sources of information to conduct the review.

Agencies should pay particular attention to the types of information that is being shared; the purpose(s) for which the information is shared; the frequency with which it is shared; and the rules (if any) regarding the retention, re-disclosure, and destruction of Federally-supplied information by the State, local or tribal governments. In conducting this review, agencies shall
evaluate whether each collection or disclosure continues to be appropriate and consider whether adequate confidentiality and security safeguards apply. In this regard, "changes in technology, function, and organization" (whether at the Federal level or at the State, local or tribal level) may render outdated the sharing of certain types of information (or the frequency of sharing), or may result in applicable safeguards being inadequate (or inadequately implemented).

Based on these reviews, agencies should identify any potential changes to information sharing practices that deserve further review. Agencies should address, including through discussions with their governmental counterparts, whether and how such potential changes should be made.

6. Report to OMB.

After completing the review outlined above, each agency should summarize its findings in a report to OMB, as described below.

a. What should the report contain?

Each agency's report should include the following:

a. A certification by the agency's Chief Information Officer and the agency's Senior Official for Privacy Policy designated under section **B.1.** of these instructions, that the review was conducted.

b. A summary of the actions taken as a result of the review, including citations to the Federal Register notices of any issuances of, or revisions to, systems of records notices.

c. A summary of future actions that the agency plans to take as a result of the review to assure sound privacy practices across the agency, and a schedule of when those actions will be completed.

d. A summary of the agency's review of its routine uses, including, in particular, the extent to which the agency found that its routine uses remain justified and compatible with the purpose for which the information was collected.

e. A description of the agency's major information sharing practices with State, local and tribal governments, including in particular whether the review identified potential changes to sharing practices that will undergo further review (and if so, a description of such potential changes).

f. Any subjects on which the agency would like further OMB guidance on the Privacy Act, and any recommendations regarding such guidance.

b. When is the deadline for reporting?

With the exception of the designation of the Senior Official for Privacy Policy in **B.1.**, which should be made immediately, the report in **B.6.** should be made to OMB by May 14, 1999.

c. To whom should the report be addressed?

Director
Office of Management and Budget
Attention: Docket Library
Room 10201 NEOB
725 17th Street, NW
Washington, DC 20503

D. WHO CAN ANSWER QUESTIONS ABOUT THIS MEMORANDUM?

For more information regarding these instructions, contact:

Maya A. Bernstein
Senior Policy Analyst
Information Policy and Technology Branch
Office of Information and Regulatory Affairs
725 17th Street, NW
Washington, DC 20503

202/395-3785 (voice)
202/395-5167 (facsimile)

Maya_A._Bernstein@omb.eop.gov