GAO
Accountability * Integrity * Reliability

GAO's Report on the Privacy Act

Presentation to Information Security and Privacy Advisory Board

Linda Koontz
Director, Information Management Issues

December 17, 2004

We recently issued a report on the results of a review of the compliance of federal agencies with the Privacy Act. We undertook this review at the request of Congress.

> U.S. General Accounting Office, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304, June 30, 2003.

Objectives: To determine

- Key characteristics of systems of records reported by agencies
- The level of agency compliance with the Privacy Act and related OMB guidance
- The extent to which agencies report that they maintain personal information that is not subject to the Privacy Act's protections

System of records

- A collection of information about individuals
- Under the control of an agency
- From which information is retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual

Personal information:

- All information associated with an individual, both *identifying* and *nonidentifying*:
  - Identifying information can be used to locate or identify someone
    - **Identifying:** name, aliases, social security number, e-mail address, drivers license identification number, agency-assigned case number
    - **Nonidentifying:** age, education, finances, criminal history, physical attributes, gender

Method

- Performed three surveys at 25 departments and agencies:
  - Agencywide practices
  - Sample of systems of records
  - Information outside Privacy Act systems of records
    - Response rates of 76 to 100 percent
- Solicited documentation or explanations for a random sample of responses to the surveys
- Convened a forum of agency Privacy Act officers

- Most systems of records contained electronic records, and systems were very diverse:
  - people covered: 5 people to 290 million (median 3,500)
  - systems per agency: 1 to over 1,000 (median 68)
- Agency compliance generally high but uneven for the various provisions, ranging from 100 percent to about 70 percent
- Agencies maintained personal information that was not subject to the Privacy Act's protections in an estimated 11 percent of 730 major information systems in use during fiscal year 2002.

- The Privacy Act of 1974 is the primary act that regulates the federal government's use of personal information.
- Major provisions of the Privacy Act:
  - Collecting only necessary information.
  - Providing public notice.
  - Providing for informed consent.
  - Protecting against adverse determinations through maintaining accuracy of personal information.

- Safeguarding information.
- Accounting for disclosures of records.
- Training employees.
- Providing notice of exemptions of systems of records.
- Providing for civil remedies and criminal penalties for violating the rights granted by the Privacy Act.

1988 Computer Matching and Privacy Protection Act

- Amended the Privacy Act
- Requires a written computer matching agreement for any computerized comparison of automated systems of records for determining the eligibility for federal benefits or for recouping payments or debts under federal benefits programs
- Agreements also required for computerized comparison of federal personnel or payroll systems

Key Characteristics

Most Systems of Records Contain Electronic Records

- 70 percent of the agencies' 2,400 systems of records contain electronic records.
  - 12 percent exclusively electronic
  - 58 percent a combination of paper and electronic
  - 31 percent exclusively paper
- Agencies allowed individuals to access their personal information via the Internet in an estimated 9 percent of systems of records (about 1 in 10).

- Great diversity of systems:
  - People covered by a systems of records: 5 people to 290 million (median 3,500)
  - Systems per agency: 1 to over 1,000 (median 68)
- Among electronic records:
  - 66 percent of systems of records resided within one information system
  - 34 percent resided within more than one information system

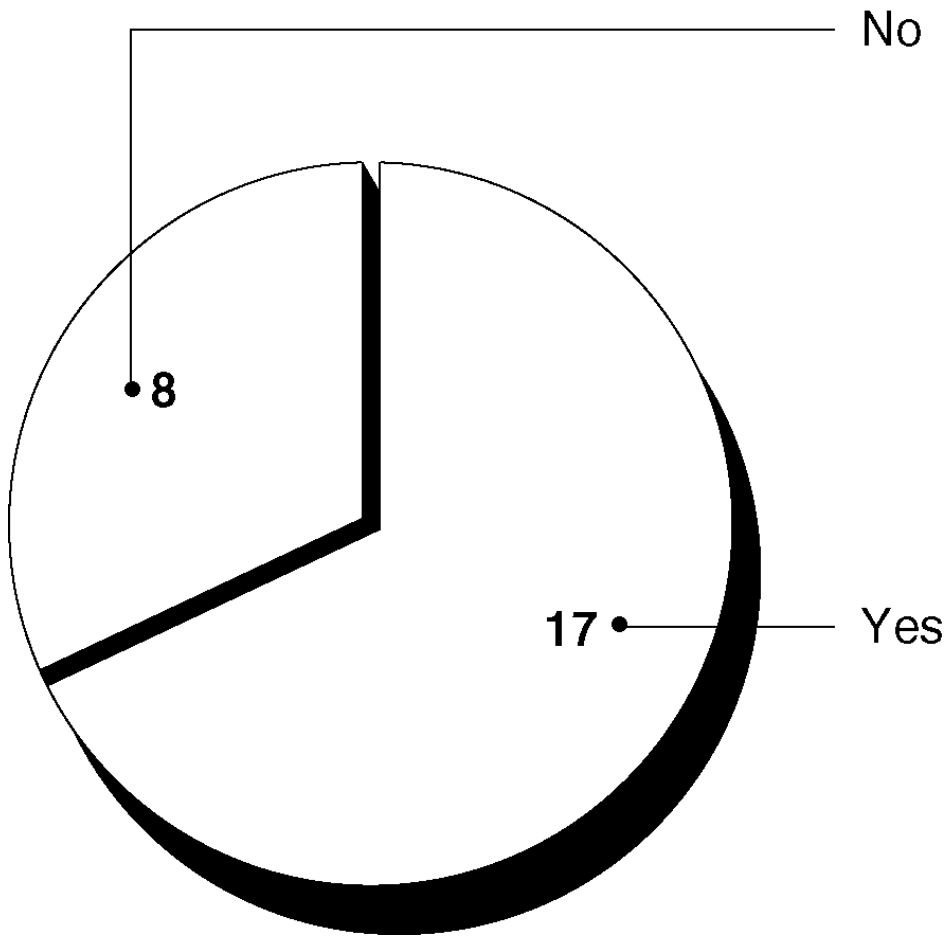
- Information used most frequently to retrieve personal information
  - Social security number
  - Agency identification number
- Source of the personal information in the systems of records:
  - Most frequent: subject individual
  - Then the agency, individuals other than the subject, and another federal agency

Compliance with Provisions of the Privacy Act

Collecting Only Relevant and Necessary Information

Survey question:

Before [new] systems become operational, does your agency have written policies or procedures for determining whether that personal information is needed?



Source: GAO.

Agencies with such procedures reported positive results:

Transportation	Reduced the amount of personal information and its availability in two systems
The Treasury	Decided not to collect or retain social security numbers in two systems
Social Security Administration	Decided not to copy two systems because it would need to access only a small percentage of the records
Department of Defense	Eliminated database information on dependents after finding that the information was neither relevant nor necessary Destroyed employees' tax return information because it was neither relevant nor necessary

The Privacy Act requires agencies to

1. issue Federal Register notices so that there are no systems of records whose existence is secret and
2. publish rules in the Code of Federal Regulations that describe the agency's procedures for individuals to determine if they are the subject of a record and to access or amend their records.

OMB Circular A-130 requires agencies to review each system of records notice biennially to ensure that it accurately describes the system of records.

According to agency responses:

- Agencies had issued the required Federal Register notice for 89 percent of the systems of records.
- 24 of 25 agencies had published the required rules in the Code of Federal Regulations.
- Agencies had completed reviews of Federal Register notices on an estimated 79 percent of the 2,400 systems of records.

- Agencies must provide individuals in writing
  - the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary,
  - the principal purposes for which the information is intended to be used,
  - the routine uses that may be made of the information, and
  - the effects on the individual, if any, of not providing the information.
- Agencies must review routine use disclosures to ensure that they continue to be appropriate.

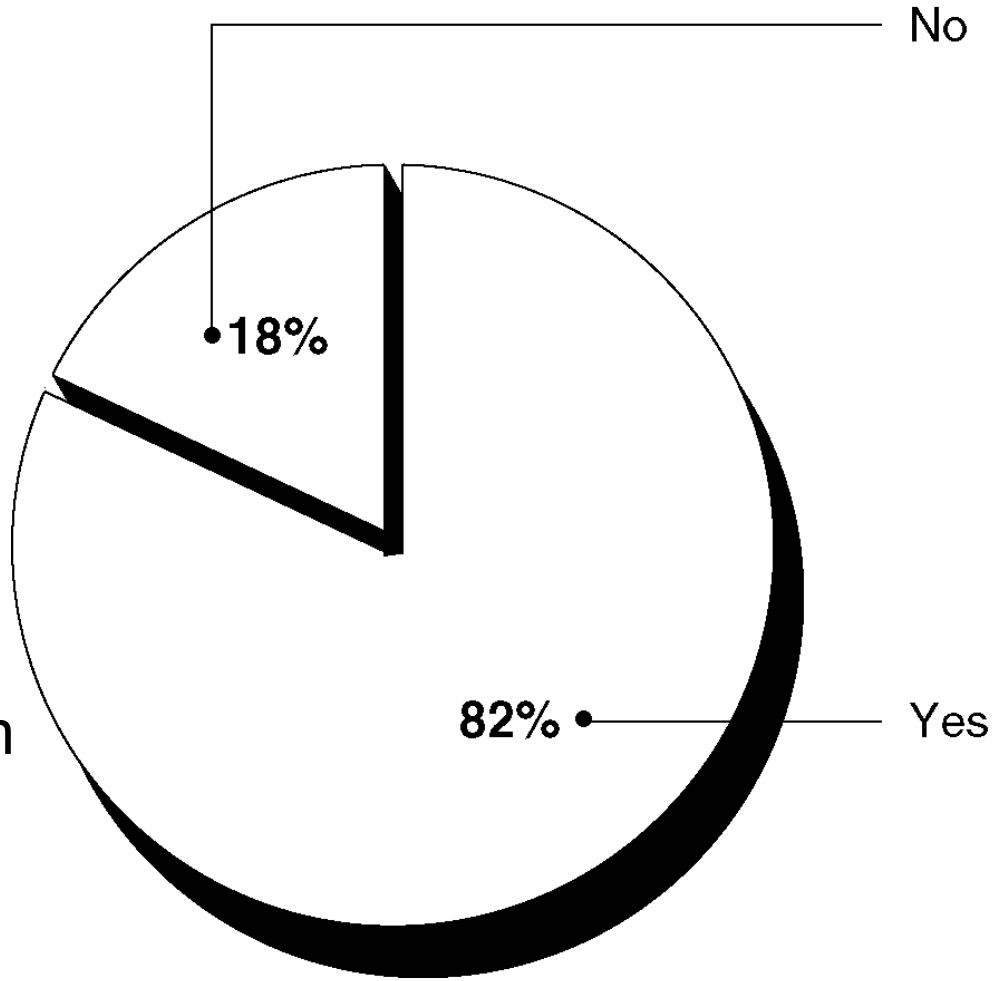
- Required information
  - Provided for 82 percent of the systems of records
- Review of routine use disclosures
  - 21 of 25 agencies had reviewed routine use disclosures
  - agencies reviewed these routine use disclosures in an estimated 82 percent of the 2,400 systems of records

- When making determinations about individuals or when disclosing personal information to a nonfederal organization, agencies must maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness.
- When making determinations, agencies had procedures in place to ensure accuracy of personal information in 95 percent of systems of records.
- When disclosing personal information, such procedures were in place for 71 percent of systems of records.

- For computer matches subject to the Privacy Act, a written computer matching agreement is required.
- OMB requires agencies to review computer matching programs for compliance with the Privacy Act and OMB guidance.
  - Less than 5 percent of ~2,400 systems of records were involved in computer matching programs in 2001.
    - This 5 percent includes very large systems (e.g., one covering ~360 million applicants for social security numbers).
    - 9 of the 13 agencies with such programs complied with the OMB requirement for review.

Survey question:

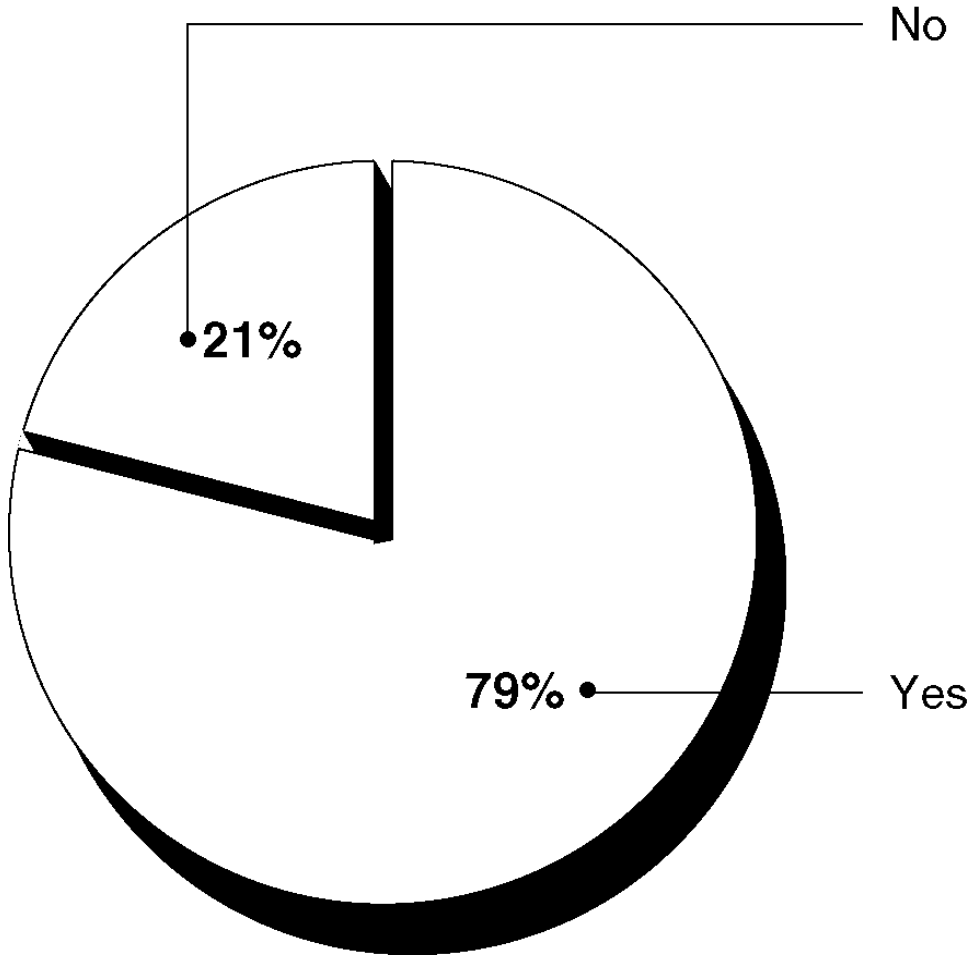
At any time during fiscal years 1999–2001, did your agency assess the threats, vulnerabilities, and effectiveness of current or proposed safeguards for the automated information system in which this system of records resides?



Source: GAO.

Survey question:

Since October 1, 2000, did your agency have the means to detect when persons, without authorization, were reading, altering, disclosing, or destroying information in this automated information system?



Source: GAO.

- Agencies are to maintain an accounting of the date, nature, and purpose of each disclosure of a record, and the name and address of the person or agency to whom the disclosure is made.
- Agencies were able to account for such disclosures in 86 percent of their 2,400 systems of records but were not able to do so for 14 percent.

Compliance question	In compliance
Has your agency established rules of conduct for persons who are involved in operations and maintenance of records?	16 of 24 agencies
Has your agency established rules of conduct for persons involved in design and development of systems of records?	15 of 24 agencies
Does your agency have procedures to ensure that personnel with access to systems of records or who are engaged in developing procedures are adequately trained?	20 of 25 agencies

Source: GAO.

- For 74 percent of systems of records, agencies provided “all or almost all” staff with Privacy Act training but did not for 26 percent.

The Privacy Act contains two categories of exemptions:

1. general exemptions (systems of records maintained by the Central Intelligence Agency or for criminal law enforcement purposes) and
2. specific exemptions (systems of records that include classified material, statistical records, and certain personnel investigation and evaluation material).

- No exemptions are automatic.

- To exempt a system from any requirement of the act,
  - a determination must be made that the system falls into one of the two categories of systems permitted and
  - a notice must be published.
    - The notice must include why the exemption is necessary and the specific provisions exempted.
- Agencies must review exemptions every 4 years.
- The following table show our estimates of compliance with these requirements and guidance.

Compliance with Provisions of the Privacy Act
Providing Notice of Exemptions

Compliance question	Results
Has your agency issued a *Federal Register* notice explaining the reasons for exempting the system of records from certain provisions of the act?	24 of 24 agencies in compliance
During fiscal years 1998–2001, did your agency review each system of records containing exemptions to determine whether such exemptions were still needed?	19 of 24 agencies in compliance
Has your agency issued a rule that explains why your agency considers the exemption necessary?	100 percent compliance among systems of records
During fiscal years 1998–2001, did your agency review the exemptions to determine whether these exemptions were still needed?	85% of systems of records in compliance;[a] 15% not in compliance

Source: GAO.

[a] The confidence interval is ±15 percent.

- At our forum, Privacy Act officers from the agencies saw the following as most significant barriers to improved compliance:
  - lack of sufficient OMB leadership, oversight, and guidance on the Privacy Act
  - low agency priority on implementing the act, which adversely affects the level of resources devoted to it
  - insufficient training to satisfy the wide range of employee involvement with the act

Barriers to Compliance: Insufficient OMB Attention

- Most agencies judged OMB's overall assistance on the act to be at least "moderately effective."
  - However, they wanted further guidance in specific areas, such as electronic records.
- Agencies want OMB to become more proactive:
  - publishing additional guidance in certain areas
  - providing increased assistance to agencies
  - convening periodic meetings of Privacy Act officers to discuss important areas where the guidance is not clear

Barriers to Compliance: Insufficient OMB Attention

- Specific additions or revisions to OMB guidance cited most frequently:
  - how the definition of a system of records applies to electronic databases
  - how the disclosure provisions apply to electronic databases
  - coverage of sole proprietors (entrepreneurs)
  - cost-benefit guidance for computer matches

- Implementation of the Privacy Act often low priority at agencies
  - A support function; often first to be cut when resources are tight
  - Privacy Act offices often “buried” in agencies
  - Privacy Act officers may be bearers of bad news: telling management that certain actions could violate the act.
- Agencies see OMB as giving low priority to Privacy Act
  - One person at OMB devoted to assisting agencies to carry out the act

- Privacy Act officers believe low priority adversely affects resources assigned to implementation.
- To address this barrier, they would have agency managers place increased priority on implementing the act
  - including making additional resources available.
- However, most agencies were unable to answer survey questions on resources that are devoted to implementing the act. Agencies are not required to track such resources, and many respondents found estimating the resources burdensome.

- According to forum participants, agencies did not provide sufficient training for agency staff who handle personal information subject to the act.
- To address this barrier, OMB should
  - oversee the development of additional training for employees involved with the act,
  - make the training more readily available (e.g., Web, CD),
  - make training role-based—according to employees' varying degrees of involvement with the act (for example, executives, Privacy Act officers, and systems managers).

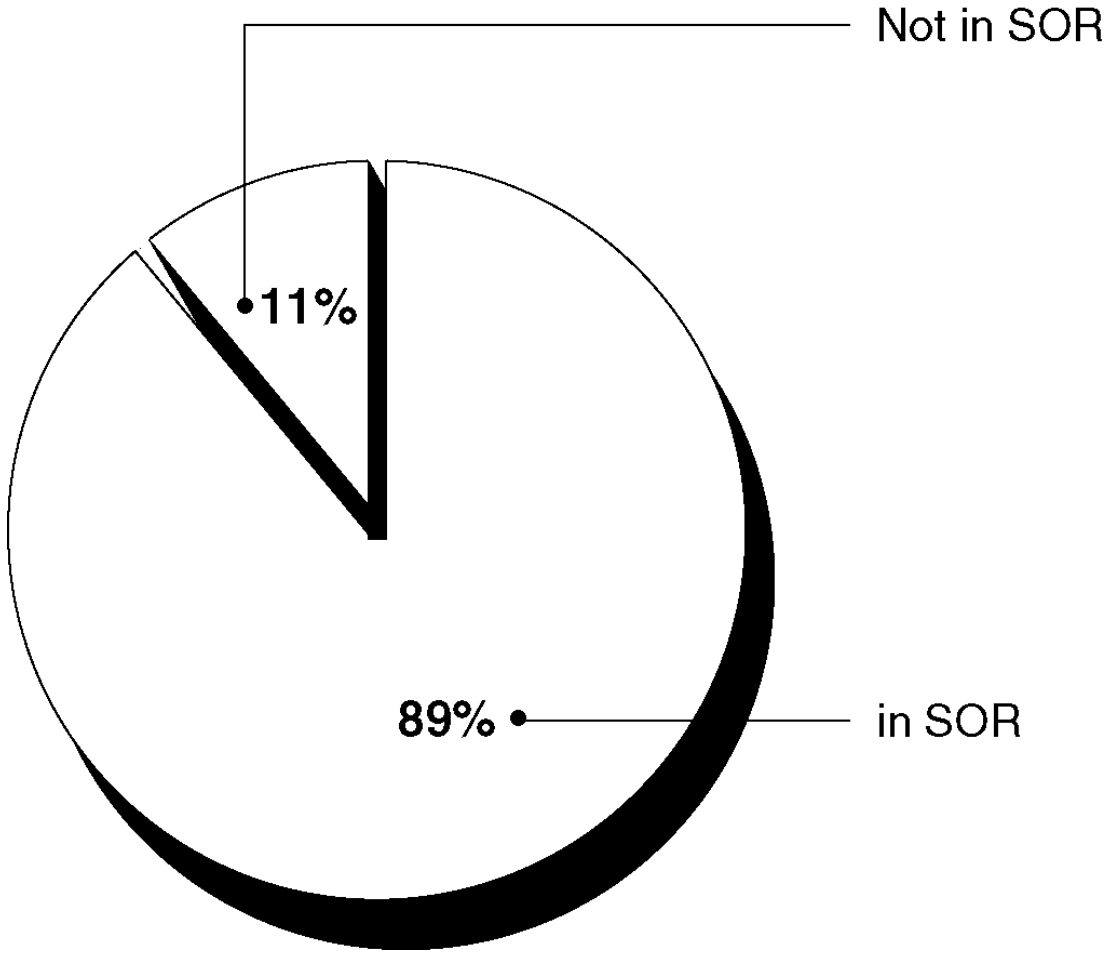
Based on our survey, we estimated the extent of personal information maintained outside Privacy Act systems.

- 67 percent of the 730 information systems in use at large agencies during fiscal year 2002 contained personal information, regardless of whether this personal information was in a Privacy Act system of records.
- Of these 730, we estimate that 11 percent (83) contained personal information outside a Privacy Act system of records.

Personal Information outside the Privacy Act

Survey question:

How many of these information systems contain any personal information not in a Privacy Act system of records (SOR)?



Source: GAO.

- Personal information is maintained outside a Privacy Act system of records when it
  - is not retrieved by use of identifying information (e.g., name), but by nonidentifying information (e.g., zip code);
  - concerns deceased persons (e.g., deceased recipients of social security benefits);
  - concerns entrepreneurs acting in a business rather than a personal capacity (e.g., persons seeking government business loans); or
  - concerns aliens who are not permanent residents of the United States (e.g., persons seeking a visa to enter this country).

- The most frequently cited reason why systems were not considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the personal information.
  - For example, the Department of Labor collects personal information from persons who claim not to have been paid all the wages owed them. Because it uses company names, rather than the names of individuals, to retrieve the information, Labor officials stated they are not required to keep this personal information in a Privacy Act system of records.

- Other laws provide privacy and security protections to personal information outside Privacy Act systems of records.
  - Two exemptions in the Freedom of Information Act protect personal privacy interests from disclosure:
    - Certain personnel and medical files
    - Certain law enforcement information
  - The Federal Information Security Management Act (FISMA) requires federal agencies to protect agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Conclusions

- Federal agencies operate in an increasingly complex environment.
  - largely electronic systems covering vast numbers of individuals
  - single system of records may reside in multiple information systems.
- Understanding this environment will be important as the government refines its privacy policies and guidance.
- Privacy Act compliance is generally high, but it is not consistent and could be improved.
- Without improved compliance, the government cannot assure the public that individual privacy rights are protected.

- To improve agency compliance, we recommended that the Director, OMB,
  - direct agencies to correct the identified deficiencies in compliance with the Privacy Act,
  - oversee implementation of actions to correct these deficiencies, and
  - monitor overall agency compliance with the act.

- To address implementation issues, we recommended that the Director
  - assess the need for specific changes to OMB guidance (especially with regard to electronic records) and update it as appropriate;
  - raise the awareness and commitment of senior agency officials to the importance of the principles that underlie the Privacy Act;

- lead a governmentwide effort to (1) determine the level of resources, including human capital, currently devoted to Privacy Act implementation by both OMB and the agencies, (2) assess the level of resources needed to fully implement the act, (3) identify the gap, if any, between current and needed resources, and (4) develop a plan for addressing any gap that may exist; and
- oversee the development of Privacy Act training that meets the needs of the wide range of employees who carry out the act and make this training readily available to agencies.

- Further, we recommended that the Director oversee an assessment of the potential impact on individual privacy of federal agencies' maintaining personal information that is not subject to the act.

Comments from OMB

- OMB sees our report as an “important first step” toward identifying areas for further research. However:
  - Information presented does not support the conclusion that without improved compliance, the government cannot assure the public that individual privacy rights are being protected.
  - It is a fundamental flaw to treat all provisions of the act as equally important in protecting privacy.
  - Lack of perfect consistency is “hardly surprising” across the dozens of agencies that make up the government.
  - Recommendations are vague and nebulous.

OMB Actions

- Since report was issued, OMB has convened at least one meeting of Privacy Act officers.