United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

June 2003

PRIVACY ACT

OMB Leadership Needed to Improve Agency Compliance

GAO-03-304

June 2003

PRIVACY ACT

OMB Leadership Needed to Improve Agency Compliance

GAO Accountability • Integrity • Reliability
Highlights

Highlights of GAO-03-304, a report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

Why GAO Did This Study

The Privacy Act regulates how federal agencies may use the personal information that individuals supply when obtaining government services or fulfilling obligations—for example, applying for a small business loan or paying taxes. GAO was asked to review, among other things, agency compliance with the Privacy Act and related guidance from the Office of Management and Budget (OMB).

What GAO Recommends

GAO recommends that the Director, OMB, take a number of steps aimed at improving agency compliance with the Privacy Act, including overseeing and monitoring agency actions, reassessing the need for additional guidance to agencies, and raising agency awareness of the importance of the act. In providing comments, OMB officials stated that the draft report does not support the conclusion that, without improved compliance, the government cannot ensure the protection of individual privacy rights; these officials stated that GAO's treatment of the various provisions of the act as equally important in protecting privacy is flawed. GAO's view, however, is that Congress enacted a series of requirements designed, in total, to protect privacy; accordingly, GAO based its conclusions on a comprehensive analysis of agency compliance with a broad range of requirements.

www.gao.gov/cgi-bin/getrpt?GAO-03-304.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Based on responses from 25 selected agencies to GAO surveys, compliance with Privacy Act requirements and OMB guidance is generally high in many areas, but it is uneven across the federal government. For example, GAO used agency responses to estimate 100 percent compliance with the requirement to issue a rule explaining to the public why personal information is exempt from certain provisions of the act (see table). In contrast, GAO estimates 71 percent compliance with the requirement that personal information should be complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization. As a result of this uneven compliance, the government cannot adequately assure the public that all legislated individual privacy rights are being protected.

Agency senior privacy officials acknowledge the uneven compliance but report a number of difficult implementation issues in a rapidly changing environment. Of these issues, privacy officials gave most importance to the need for further OMB leadership and guidance. Although agencies are not generally dissatisfied with OMB's guidance on the Privacy Act, they made specific suggestions regarding areas in which additional guidance is needed, such as the act's application to electronic records. Besides these gaps in guidance, additional issues included the low agency priority given to implementing the act and insufficient employee training on the act. If these implementation issues and the overall uneven compliance are not addressed, the government will not be able to provide the public with sufficient assurance that all legislated individual privacy rights are adequately protected.

Examples of Compliance with Requirements of the Privacy Act

Requirement	Compliance estimates
Issuing a rule that explains why the agency considers an exemption necessary	100% compliance
Being able to account for all disclosures of individual's records outside the agency	86% compliance; 14% not in compliance
Reviewing routine disclosures of information outside the agency to ensure that these continue to be compatible with the purpose for which the information was collected (fiscal years 1998–2001)	82% compliance; 18% not in compliance
Before disclosing records to a nonfederal organization, ensuring that the information is complete, accurate, relevant, and timely	71% compliance; 29% not in compliance

Source: GAO.

Note: Agency response rates to compliance surveys ranged from 76 to 100 percent. To give greater assurance about the accuracy of agency responses, GAO verified a random sample of responses.

Contents

Tables

Figures

Abbreviations

CIO	chief information officer
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTE	full-time equivalent
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SSA	Social Security Administration
SOR	system of records

Contents

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

June 30, 2003

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Dear Senator Lieberman:

Obtaining government services or fulfilling government obligations—for example, applying for a small business loan or paying taxes—often requires individuals to provide federal agencies with detailed personal information about themselves and their spouses, dependents, and parents.[1] To regulate the federal government's use of this personal information, Congress passed the Privacy Act of 1974. You asked us to evaluate the compliance of federal agencies with the Privacy Act and other issues. Specifically, as agreed with your office, our objectives were to determine

- key characteristics of systems of records[2] reported by agencies;
- the level of agency compliance with the Privacy Act and related OMB guidance; and
- the extent to which agencies report that they maintain personal information that is not subject to the Privacy Act's protections.

[1]Under the Privacy Act, personal information is all information associated with an individual and includes both identifying information and nonidentifying information. Identifying information, which can be used to locate or identify an individual, includes name, aliases, social security number, E-mail address, driver's license identification number, and agency-assigned case number. Nonidentifying personal information includes age, education, finances, criminal history, physical attributes, and gender.

[2]A system of records is 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.

To address these objectives, we conducted three surveys at 25 departments and agencies, which were selected to provide a cross section of large and small agencies[3] that were likely to have different missions and organizational structures and, perhaps, different approaches to implementing the Privacy Act. (App. I identifies the 25 agencies.) Response rates ranged from 76 to 100 percent.[4] To help verify the accuracy of answers related to compliance with the Privacy Act, we randomly selected a sample of agencies' responses to the surveys and asked officials to provide documentation or additional narrative explanations to support their answers for key compliance questions. The results of the verification work gave us greater assurance about the accuracy of agencies' survey responses. We previously briefed your staff on the results of our surveys.

To better understand the results of our surveys, we invited the 25 agencies to send a representative (mostly Privacy Act officers) to a meeting in February 2003 (also referred to as the "forum"), at which we presented our survey results and asked the agency representatives for their reactions and to identify barriers to compliance with the act. (A summary of forum results is presented in app. II.)

Further details on our scope and methodology are provided in appendix I. Our work was conducted from May 2001 to May 2003 in accordance with generally accepted government auditing standards.

[3]We use the term "agency" in this report to refer to executive departments such as the Department of Justice as well as independent agencies such as the Office of Personnel Management (OPM).

[4]We used three surveys to obtain information on the following areas (see app. I): the first addressed agencywide practices, and the second addressed systems of records; these two surveys addressed characteristics of systems of records and compliance with the act and related OMB guidance. The third survey focused on information technology projects; for these, we obtained information on systems containing personal information not subject to the act's protections. All percentage estimates in this report have confidence intervals of ±10 percentage points or less (unless otherwise noted) at the 95 percent confidence level. In other words, if all the systems of records in our population had been in the second survey, the chances are 95 out of 100 that the result obtained would not differ from our sample estimate by more than ±10 percentage points.

Results in Brief

Based on survey responses, a key characteristic of agencies' 2,400 systems of records is that an estimated 70 percent of systems contained electronic records. Specifically, 12 percent were exclusively electronic records, 58 percent were a combination of paper and electronic, and 31 percent were exclusively paper records.[5] In addition, we estimate that agencies allowed individuals to access their personal information electronically via the Internet in about 1 of every 10 systems of records. Other key characteristics reflected the diversity of systems: for example, the number of people whose personal information was maintained in the sampled systems of records varied significantly, from 5 people to about 290 million, with a median of about 3,500. The number of systems per agency also varied significantly: from 1 to over 1,000, with a median of 68.

While compliance with Privacy Act provisions and related OMB guidance was generally high in many areas, according to agency reports, it was uneven across the federal government—ranging from 100 percent to about 70 percent for the various provisions. For example, we estimate that for all systems of records (100 percent), agencies issued the required rule that explains to the public why they exempted the system of records from one or more of the act's privacy protections. In contrast, fewer agencies were compliant with the provision that information should be complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization; we estimate that agencies took steps to comply with this requirement for 71 percent of systems of records. At the forum, agency privacy officials acknowledged the uneven compliance but reported a number of difficult implementation issues in a rapidly changing environment. Of these issues, privacy officials gave most importance to the need for further OMB leadership and guidance. Although agencies are not generally dissatisfied with OMB's guidance on the Privacy Act, they made specific suggestions regarding areas in which additional guidance was needed, such as the act's application to electronic records. Besides these gaps in guidance, additional implementation issues included the low agency priority given to implementing the act and insufficient employee training on the act. If these issues and the overall uneven compliance are not addressed, the government will not be able to provide the public with sufficient assurance that individual privacy rights are appropriately protected.

[5] Figures do not add to 100 percent due to rounding.

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. Agencies reported that this occurred in various circumstances, the most frequent being when information was not retrieved by use of identifying information (e.g., name), but rather by other, nonidentifying information (e.g., name of a company). Concerns have been raised regarding the scope of the Privacy Act, whose coverage is limited to personal information that is retrieved by a personal identifier. Our study results are relevant to one aspect of this issue, as they provide an indication of the extent to which agencies maintain personal information not subject to the act's protections. A more complete examination of this topic would require additional study.

To improve compliance and address issues reported by agencies, we are making recommendations to the Director, OMB, which include directing agencies to correct compliance deficiencies, monitoring agency compliance, and reassessing OMB guidance.

In commenting on a draft of this report, the Administrators of OMB's Offices of Information and Regulatory Affairs and of E-Government and Information Technology stated that the information in the draft report does not support our conclusion that, without improved compliance, the government cannot assure the public that individual privacy rights are being protected. Specifically, the Administrators fault what they characterize as a fundamental flaw in the draft report: our treatment of the various provisions of the act as equally important in protecting privacy. In addition, OMB disagrees with our recommendations, stating that they are vague and nebulous.

We disagree with OMB's assertion that our conclusion is not supported. We continue to believe that, without improved compliance, the government cannot adequately assure the public that all legislated individual privacy rights are being protected. In enacting the Privacy Act, Congress established a framework for ensuring that individuals' privacy is protected. Accordingly, we based our conclusions on a comprehensive analysis of agency compliance with a broad range of requirements contained in the act. With regard to our recommendations, the report contains considerable detail including specific compliance results and agency suggestions for improvements to OMB guidance. In addition, we believe that our recommendations provide the appropriate level of detail needed for OMB to address the issues from a governmentwide perspective. However, we recognize that the compliance results in particular are provided in

aggregate form; we will be providing additional details to OMB to help it in improving governmentwide compliance.

Background

The Privacy Act of 1974 is the primary act that regulates the federal government's use of personal information. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information in systems of records. A system of records is a collection of information about individuals under the control of an agency from which information is actually retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual. The act does not apply when there is merely a capability or potential for retrieval by identifier, which is often the case with electronic records.

Among the major provisions of the Privacy Act are the following:

Collecting only necessary information. Agencies are to maintain personal information about an individual only when it is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. According to OMB guidance, the goal of this provision is to reduce the amount of personal information that agencies collect in order to reduce the risk of agencies' improperly using personal information.

Providing public notice. Agencies are to publish a notice in the *Federal Register* when establishing or revising a system of records. The notice is to contain the name and location of the system, the categories of individuals on whom records are maintained in the system, and each "routine use"[6] of the records contained in the system.

Providing for informed consent. Agencies are to inform individuals whom it asks to supply information of (1) the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary, (2) the principal purposes for which the information is intended to be used, (3) the routine uses that may be made of the information, and (4) the effects on the individual, if any, of not providing the information.

[6]Under the act, a routine use is a disclosure of personal information outside the agency maintaining the information that the agency determines is compatible with the purpose for which it was collected.

Protecting against adverse determinations through maintaining accuracy of personal information. Agencies are to maintain all records used in making any determination about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Safeguarding information. Agencies are to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Accounting for disclosures of records. Agencies are to keep 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 (except for disclosures within the agency for official purposes or for disclosures required under the Freedom of Information Act).

Training employees. Agencies are to instruct persons on the requirements of the act if they are involved in the design, development, operation, or maintenance of any system of records or in maintaining any record.

Providing notice of exemptions of systems of records. When an agency uses the authority in the act to exempt a system of records from certain provisions, the agency is to issue a rule explaining the reasons for the exemption.

Providing for civil remedies and criminal penalties for violating the rights granted by the Privacy Act. The act grants individuals the right of access to agency records pertaining to themselves; the right to amend such a record if it is inaccurate, irrelevant, untimely, or incomplete; and the right to sue the government for violations of the act. There are civil remedies and criminal penalties for agencies not affording individuals these rights.

In 1988, Congress amended the Privacy Act through passage of the Computer Matching and Privacy Protection Act, which established safeguards regarding an agency's use of Privacy Act records in performing certain computerized matching programs. Under the act, a written computer matching agreement is required for any computerized comparison of two or more automated systems of records for the purposes

of determining the eligibility of applicants for assistance under federal benefits programs or of recouping payments or delinquent debts under federal benefits programs. Agreements are also required for any computerized comparison of federal personnel or payroll systems.

Computer matching agreements must specify the purpose and legal authority for conducting the match and how these matches will be performed. Agency Data Integrity Boards are to approve matching agreements and assess the costs and benefits of the match. (There are some exceptions, such as not assessing costs and benefits where the match is required by statute.)

OMB Is Responsible for Guidance on Privacy

Under the Privacy Act, OMB is responsible for developing guidelines and regulations and providing "continuing assistance to and oversight of" agencies' implementation of the act. In 1975, OMB issued its initial Privacy Act implementing guidance entitled *Privacy Act Implementation: Guidelines and Responsibilities.* In addition, OMB Circular A-130 (*Management of Federal Information Resources*) sets forth a number of general policies concerning the protection of personal privacy by the federal government:

- The individual's right of privacy must be protected in federal government information activities involving personal information.
- Agencies shall consider the effects of their actions on the privacy rights of individuals and ensure that appropriate legal and technical safeguards are implemented.
- Agencies shall limit the collection of information that identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions.
- Agency heads shall periodically review (1) a random sample of agency contracts for maintaining systems of records to ensure that contractors are bound by the Privacy Act; (2) routine use disclosures associated with each system of records to ensure that they are compatible with their original purpose for collection; and (3) training practices to ensure that employees are familiar with the Privacy Act and the agency's implementing regulation.

As of April 2003, OMB's Web site, www.whitehouse.gov/omb, also provides links to documents characterized as "Privacy Guidance" and "Privacy Reference Materials" (http://www.whitehouse.gov/omb/inforeg/infopoltech.html). Those documents include the initial Privacy Act guidance, memoranda about privacy policies on federal Web sites, interagency sharing of personal data, letters on agency use of Web "cookies."[7] (See app. III.)

OMB officials stated that one OMB staff person is dedicated to Privacy Act issues full time. In addition, according to that one staff person, several other OMB staff also devote part of their time to this effort. The Privacy Act staff position is located in the Information Policy and Technology Branch within the Office of Information and Regulatory Affairs. According to OMB, the duties associated with this position include

- reviewing agencies' draft *Federal Register* notices and systems reports for new and altered systems of records and computer matches;
- answering agencies' questions about how to implement the act, and responding to questions from federal employees and the public about the scope and application of the act;
- monitoring court rulings involving the Privacy Act;
- developing written guidance to agencies on Privacy Act implementation issues and federal Internet privacy policy;
- leading interagency work groups on Privacy Act issues;
- providing input to OMB's positions on legislation, rules, regulations, and testimony that have privacy policy implications; and
- participating in interagency discussions and activities concerning other privacy policy issues (consumer fraud/identity theft, do-not-call lists, medical privacy, financial privacy, etc.).

[7]A cookie is a short string of text that is sent from a Web server to a Web browser when the browser accesses a page. Certain types of cookies may pose privacy risks because they may be used to track individuals' browsing habits and keep track of viewed and downloaded pages.

One body tasked with addressing federal governmentwide issues such as privacy and security is the Chief Information Officers (CIO) Council, chaired by the Deputy Director for Management in OMB. Initially established in 1996 by Executive Order 13011, the CIO Council was enacted into law by the E-Government Act of 2002.[8] The council serves as the principal interagency forum for improving practices in the management of federal information resources. Among its functions are responsibilities to develop policy recommendations for OMB, help coordinate multiagency projects and other innovative initiatives, assist in standards development, and work with the Office of Personnel Management (OPM) to address hiring and training needs.[9]

Previous Initiatives and Studies Have Raised Privacy and Security Concerns

Concerns about implementation of the Privacy Act have arisen periodically since its passage. In 1983, for example, in a report summarizing 9 years (1975–1983) of congressional oversight of the act, the House Committee on Government Reform (formerly called the Committee on Government Operations) concluded that OMB had not pursued its responsibility to revise and update its original guidance from 1975 and had not actively monitored agency compliance with its guidance.[10] It stated "Interest in the Privacy Act at [OMB] has diminished steadily since 1975. Each successive Administration has shown less concern about Privacy Act oversight."

[8]Public Law 105-277, Div. C, tit. XVII.

[9]44 U.S.C. 3603, Public Law 107-347 (Dec. 17, 2002).

[10]House Report No. 98-455.

A subsequent administration initiative addressed the difficulty of assuring privacy in an increasingly electronic environment. In May 1998, a presidential memorandum was issued stating that increases in agencies' use of electronic records permit "this information to be used and analyzed in ways that could diminish individual privacy in the absence of additional safeguards." Consequently, the heads of executive departments and agencies were directed to review their Privacy Act systems of records within 1 year, and OMB was directed, among other things,[11] to issue instructions to agencies on conducting and reporting these reviews. In its January 1999 instructions, OMB also asked agencies to identify areas where they believe further OMB guidance was needed.[12]

The resulting responses from 72 agencies highlighted a range of issues. For example, in assessing their own compliance with the Privacy Act, agencies (1) added 131 systems of records that previously had not been properly identified, (2) revised 457 systems of records that were not up to date, and (3) deleted 288 systems of records that were no longer necessary. In addition, agencies requested centralized, updated guidance, particularly with regard to new technologies such as E-mail, Web sites, and electronic records. Further, agencies suggested, for example, that OMB establish an interagency taskforce on privacy.

[11]The President also directed OMB to summarize the results of the agency reviews. OMB officials stated that they did not do so. However, the OMB official who is responsible for overseeing the Privacy Act stated that the Presidential initiative did result in OMB urging agencies to include privacy impact assessments when preparing their budget Exhibit 300 submissions for information technology purchases. She also stated that a similar requirement for privacy impact assessments was subsequently enacted into law (P.L. 107-347).

[12]OMB Memorandum M-99-05 (Jan. 7, 1999).

In addition, over the past 3 years, we have issued reports that raised concerns with the adequacy of selected OMB guidance. In September 2000, we reported that OMB's guidance to agencies on Web site privacy policies was unclear in several respects and contained undefined language. We recommended that OMB clarify its guidance on privacy policies for agencies' Web sites.[13] In another report, issued in April 2001, we said that OMB's guidance on agencies' use of cookies on Web sites was fragmented and did not provide clear direction.[14] We recommended that OMB clarify its guidance. Although OMB officials stated that they planned to address these recommendations, OMB had not yet implemented them as of May 2003.

We have also consistently reported that security of electronic information in computer systems is a high-risk area for the government in general, with potentially devastating consequences if it is not ensured. When controls over the security of computer systems are not adequate, the privacy of the personal information in those systems is exposed to potential risks from unauthorized access or alteration. In April 2003, at the request of Congress, we testified on our analysis of recent information security audits and evaluations at 24 major federal departments and agencies.[15] We reported that although analyses of audit and evaluation reports for the 24 major departments and agencies issued from October 2001 to October 2002 indicated some individual agency improvements, overall they continued to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. We identified significant weaknesses in each of the 24 agencies. As in 2000 and 2001, weaknesses were most often identified in control areas for security program management and access controls. All 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

We further testified that there are a number of important steps that the administration and the agencies should take to ensure that information

[13]*Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO/GGD-00-191 (Washington, D.C.: Sept. 5, 2000).

[14]*Internet Privacy: Implementation of Federal Guidance for Agency Use of Cookies*, GAO-01-424 (Washington, D.C.: Apr. 27, 2001).

[15]*Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003).

security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Although we continue to report significant weaknesses that place federal operations and assets at risk, in the past few years agencies and the administration have taken actions to improve federal information security. As we reported in our April 2003 testimony, OMB and agency efforts to implement the information security requirements of the Federal Information Security Management Act (FISMA)[16] have resulted in increased management attention to information security and provided an improved baseline for measuring improvements. FISMA requires federal agencies to establish agencywide risk-based information security programs, which must be independently evaluated annually, in order to protect agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

We also reported that the administration has made progress through a number of efforts, such as OMB's establishment of requirements for agencies to report the results of their annual security program reviews and their plans to correct identified weaknesses, as well as its emphasis of information security in the budget process and e-government initiatives.[17] Also, the National Institute of Standards and Technology (NIST) has issued additional computer security guidance, including its *Security Self-Assessment Guide for Information Technology Systems*,[18] which uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured.

[16]Title III of the E-Gov Act (P.L. 107-347).

[17]E-government refers to the use of technology, particularly Web-based Internet applications, to enhance the access to and delivery of government information and services to citizens, business partners, employees, other agencies, and other entities.

[18]National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26 (November 2001).

Most Agencies' Systems of Records Contain Electronic Records

A key characteristic of agencies' systems of records is that a large proportion of them are electronic, reflecting the government's significant use of computers and the Internet to collect and share personal information. Based on survey responses, we estimate that 70 percent of the agencies' 2,400 systems of records contain electronic records. Specifically, an estimated 12 percent were exclusively electronic records, 58 percent were a combination of paper and electronic, and 31 percent were exclusively paper records.[19] In addition, agencies allowed individuals to access their personal information via the Internet in an estimated 9 percent of systems of records (about 1 in 10).

Our survey results revealed other key characteristics of our population of over 2,400 systems of records, which illustrate the diversity across agencies:

The median number of people whose personal information was maintained in the sampled systems of records was about 3,500, but this number varied significantly: the totals ranged from 5 people to about 290 million people.

- The median number of systems of records at each agency was 68, but this number varied significantly: the totals ranged from 1 to over 1,000.
- Among the electronic records, 66 percent of systems of records resided within one information system, and 34 percent resided within more than one information system.
- The types of information that agencies used most frequently to actually retrieve personal information from the system were the social security number and the agency identification number.
- The most frequent source of the personal information in the systems of records was the subject individual, followed by the agency, individuals other than the subject, and another federal agency.

[19]Figures do not add to 100 percent due to rounding.

Agency Compliance with the Privacy Act and OMB Guidance Is Uneven

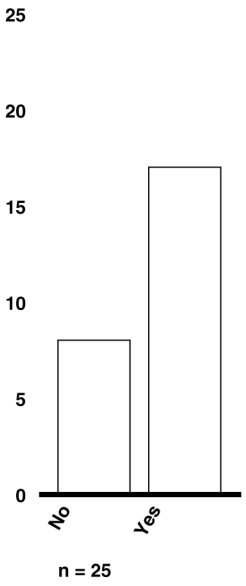
While compliance with Privacy Act provisions and related OMB guidance was generally high in many areas, according to agency reports, it was uneven across the federal government—ranging from 100 percent for some requirements to about 70 percent for others. For example, for 100 percent of agency systems of records, agencies followed the requirement to issue a rule that explains to the public why a system of records is exempt from one or more of the act's privacy protections. However, for other provisions, agencies have not consistently established the necessary policies and procedures needed to ensure compliance and followed through on required actions. Agency privacy officials attending our forum acknowledged this uneven compliance; they pointed out, however, that implementation of the Privacy Act in a rapidly changing environment presents a number of difficult issues. Specifically, these officials identified barriers to improved compliance that include a need for more OMB leadership and guidance on the act, low agency priority given to implementing the act, and insufficient training on the act. In the absence of consistent compliance with the Privacy Act, the government cannot adequately assure the public that all legislated individual privacy rights are being protected.

Compliance Was Uneven among Provisions of the Privacy Act

Collecting only relevant and necessary information. The Privacy Act states that agencies are to collect only information that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. This provision is aimed at preventing the improper use of personal information in ways that could result in substantial harm or embarrassment to individuals. OMB guidance states "In simplest terms, information not collected about an individual cannot be misused." Accordingly, OMB guidance states that agencies are to assess the relevance and need for personal information in the initial design of a new system of records or whenever any change is proposed in an existing system of records. Seventeen of the 25 agencies stated that they did have written policies and procedures to determine, before information systems become operational, whether any personal information to be collected in a new system is needed, as OMB guidance requires. (See fig. 1.) The remaining 8 agencies did not have such policies and procedures.

Figure 1: Policies to Assess Need to Collect Personal Information

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



Source: GAO.

Several agencies that did have such procedures in place reported positive results from these assessments. These agencies identified instances since October 1, 1998, where they decided not to collect or retain unnecessary personal information because of Privacy Act considerations. For example:

- Transportation took steps to reduce the amount of personal information and its availability in designing (1) a new identification system for agency employees and (2) a possible Transportation Worker Identification Credential (TWIC) and associated systems for the Transportation Security Administration. According to agency officials, TWIC was initiated at the Department of Transportation, but transferred to the Department of Homeland Security with the Transportation Security Administration on March 1, 2003.

- The Treasury's Financial Management Service decided not to collect or retain social security numbers for its Pay.gov verification[20] or for the Intra-Governmental Payment and Collections System.[21]

- The Social Security Administration (SSA) decided not to copy (1) a State Workers Compensation agency file and (2) a Veterans Benefits Administration file containing military discharge records, because SSA would need to access only a small percentage of the records.

- The Department of Defense eliminated a database that contained information on dependents after finding that the information was neither relevant nor necessary. Another component destroyed employees' tax return information because it was neither relevant nor necessary.

As these examples show, following procedures to assess the need for personal information in systems can effectively avoid privacy risks. However, without such procedures consistently in place governmentwide, agencies cannot ensure that only relevant personal information is collected from individuals.

Providing public notice. A basic objective of the act is to foster agency accountability through a system of public scrutiny. Among the provisions of the act that provide this system of public scrutiny are the act's requirements 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. In addition, over the course of a year, agencies' use of personal information in systems of records may change. Accordingly, OMB Circular A-130 requires agencies to review each system of records notice biennially to ensure that it accurately describes the system of records.

[20]Pay.gov is a service developed by Treasury's Financial Management Service that can be used by other federal agencies to allow customers to make payments electronically through the Internet. The service also includes payment-related functions, such as authenticating users and reporting back to agencies about transactions that have transpired.

[21]The primary purpose of the Intra-Governmental Payment and Collection System is to provide a standardized interagency fund transfer mechanism for federal program agencies.

Agencies reported that they had issued the required *Federal Register* notice for 89 percent of the systems of records. Of the 25 agencies surveyed, 24 reported that they had published the required rules in the Code of Federal Regulations. Finally, agencies reported they had completed reviews of *Federal Register* notices on an estimated 79 percent of the 2,400 systems of records. For those systems of records for which agencies are not complying with public notice provisions, the public cannot obtain current information on the existence of government systems that may contain personal information. Without uniform compliance with these provisions, agencies cannot consistently ensure that citizens can exercise their rights to access, review, and amend such records, as guaranteed under the act.

Providing for informed consent. Under the act, individuals have a right to be provided with detailed information about the agency's request for personal information before making an informed decision whether to respond. Accordingly, the act requires agencies to provide individuals in writing (1) the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary, (2) the principal purposes for which the information is intended to be used, (3) the routine uses that may be made of the information, and (4) the effects on the individual, if any, of not providing the information. In addition, agencies' uses of the information may change over time. Accordingly, OMB Circular A-130 requires agencies to review the routine use disclosures to ensure that they continue to be compatible with the purpose for which the information was collected.

We estimate that for 82 percent of the systems of records, agencies did provide individuals, in writing, with the information required by the act. For the remaining 18 percent, individuals have not been provided with full disclosure of the potential uses of their personal information.

In addition, of 25 agencies surveyed, 21 reported that they had adhered to the OMB guidance to review routine use disclosures. Based on responses to our survey of systems of records, we found that agencies reviewed these routine use disclosures in an estimated 82 percent of the 2,400 systems of records. For the systems for which these reviews were not done, agencies cannot assure the public that the potential uses of their personal information remains appropriate.

Protection against adverse determinations through maintaining accuracy. One purpose of the act is to minimize, if not eliminate, the risk

that an agency will make an adverse determination about an individual on the basis of incorrect information. Accordingly, the act requires that agencies, when making determinations about individuals or when disclosing personal information to a nonfederal organization, maintain all records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Agency-reported compliance with the accuracy requirements varied considerably. With regard to determinations made about an individual, we estimate that agencies had procedures in place to ensure that the personal information about an individual is complete, accurate, relevant, and timely in 95 percent of systems of records. However, compliance with accuracy requirements was considerably lower when the agencies disclosed personal information to nonfederal organizations—an estimated 71 percent of systems of records.

A related issue is the use of computer matches,[22] which are generally subject to the act's protections if they are used to make determinations that involve (1) applying for federal benefits, (2) recouping government payments to individuals, (3) collecting delinquent debts the individual owes the government, or (4) federal personnel or payroll records. We estimate that less than 5 percent of the approximately 2,400 systems of records were involved in one or more computer matching programs during 2001; however, this 5 percent includes systems containing records on very large numbers of people, including one, according to SSA, covering approximately 360 million applicants for social security numbers of which 70 million are known to be deceased. OMB requires agencies to review each ongoing computer matching program to ensure that the requirements of the act and OMB guidance had been met. Our survey results indicate that 9 of the 13 agencies that maintain computer matching programs complied with the OMB requirement to make such reviews.

[22]Computer matching is the identification of similarities or dissimilarities in data found in two or more computer files. However, many computer matches fall outside the act, such as matches performed to produce aggregate statistical data without any personal identifiers and matches performed to support any research or statistical project. According to OMB guidance, such data may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals. (Dec. 20, 2000, memorandum from the Director, OMB, to the heads of executive departments and agencies, Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy.)

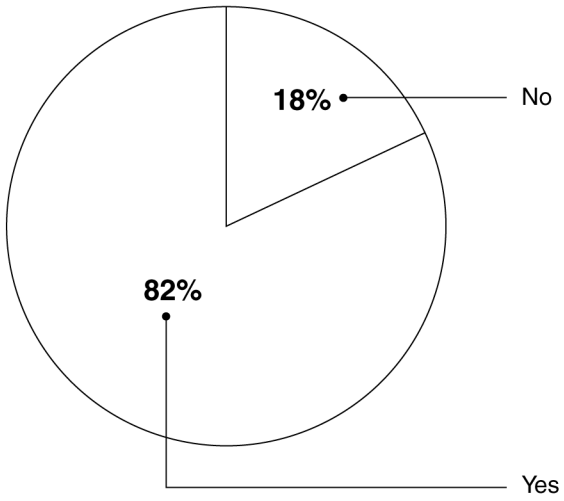
Without consistent reviews of computer matching programs for compliance with the act and OMB guidance, the government cannot ensure that personal information shared with other entities and used for decision making in federal programs is accurate, relevant, timely, and complete.

Safeguarding personal information. Once an agency makes a decision to collect personal information, safeguarding the information is vital to complying with the Privacy Act. As discussed earlier, our reports have consistently found that information security is a high-risk area for the government in general, with potentially devastating consequences if it is not ensured. Moreover, the importance of adequate safeguards is underscored by the types of sensitive personal information most frequently found in the systems of records: name, social security number, telephone numbers, home address, work address, and demographic information (e.g., marital status).

OMB's guidance calls for a detailed assessment of risks and the establishment of specific administrative, technical, procedural, and physical safeguards. Based on survey responses, we estimate that during fiscal years 1999 through 2001, agencies did assess security safeguards for 82 percent of systems of records, but did not for the remaining 18 percent. (See fig. 2.)

Figure 2: Agencies' Assessments of Security Safeguards

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?



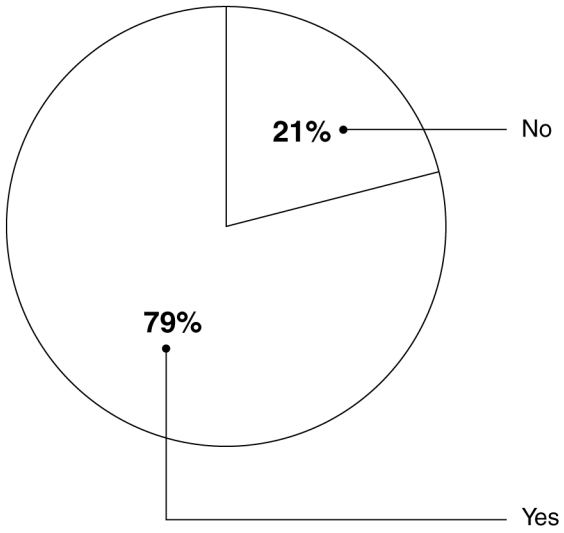
Source: GAO.

Protecting personal information that is maintained in automated information systems is of particular importance. In response to our surveys, agencies generally did not report incidents of unauthorized reading, altering, disclosing, or destroying personal information in automated information systems.[23] However, we also estimate that in 21 percent of about 2,400 systems of records, agencies reported that they did not have the means to detect when persons, without authorization, were reading, altering, disclosing, or destroying information in the system. (See fig. 3.)

[23]Agencies reported two incidents. However, these two incidents were not in our random sample and thus not weighted sufficiently to lower compliance below 100 percent, as shown in appendix IV.

Figure 3: Agencies' Means to Detect Unauthorized Access

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.

Without appropriate security safeguards and the means to assess them, agencies cannot ensure that personal information maintained by the government is protected from unauthorized access, disclosure, and alteration.

Accounting for disclosures. Individuals have a right under the act to know to whom records about themselves have been disclosed outside the agency, so that (among other purposes) those recipients can be subsequently advised of any corrected or disputed records. Accordingly, 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. We estimate that 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. For systems for which agencies cannot account for disclosures, agencies cannot advise individuals of how and by whom their personal information is being used.

Training employees. The Privacy Act states that agencies are to establish rules of conduct for persons involved in the design, development,

operation, or maintenance of systems of records and to instruct each person on those rules, including the penalties for noncompliance. In discussing the act's requirement for agencies to issue rules, OMB guidance states that training employees on the act is important for compliance:

Effective compliance with the provisions of this act will require informed and active support of a broad cross section of agency personnel. It is important that all personnel who in any way have access to systems of records or who are engaged in the development of procedures or systems for handling records, be informed of the requirements of the act and be adequately trained in agency procedures developed to implement the act.

As the table shows, one-third of agencies have not issued the act's required rules of conduct for employees, and about one out of five had not established procedures to ensure adequate training for personnel with access to systems of records.

Table 1: Agencywide Compliance with Training Requirements

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.

In addition, for an estimated 74 percent of systems of records, agencies also reported that they provided "all or almost all" staff with such training but did not for an estimated 26 percent. If agency employees have not been appropriately trained, they may not be aware of their responsibilities under the act and may not fully comply with its requirements.

Providing notice of exemptions. The Privacy Act permits certain categories of records to be exempted from some requirements of the act (e.g., access to records); according to OMB guidance, agencies can make exemptions if complying with those requirements could adversely affect agencies' conduct of necessary public business. The act contains two categories of exemptions: (1) general exemptions that include systems of

records maintained by the Central Intelligence Agency or for criminal law enforcement purposes and (2) specific exemptions for systems of records that include classified material, statistical records, and certain personnel investigation and evaluation material. For example, the act allows agencies to deny a person access to his or her law enforcement files if doing so would impair an ongoing investigation. Other types of records may be exempted from the provision in the act that allows individuals to sue for violations of the act and seek civil remedies and from the provision to ensure the accuracy of the information disclosed to third parties.

According to OMB guidance, no system of records is automatically exempt from any provision of the act. To obtain an exemption for a system from any requirement of the act, the head of the agency that maintains the system must make a determination that the system falls within one of the categories of systems that are permitted to be exempted and publish a notice on the determination as a rule. That notice must include why the agency considers the exemption necessary and the specific provisions proposed to be exempted. OMB Circular A-130 requires agencies to review any exemptions every 4 years to determine if they are still needed.

As shown in the following table, we estimate that agencies issued the required rule explaining why the system of records was exempt for 100 percent of the systems of records; however, for about one in seven systems, agencies did not review the rule every 4 years as OMB requires. For systems that are not reviewed periodically as required, agencies have diminished assurance that all existing exemptions from Privacy Act provisions are still necessary.

Table 2: Compliance with Exemption Requirements

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.

The specific compliance questions in our surveys and agency responses can be found in appendix IV.

Agencies Believe that Additional OMB Guidance Would Help Improve Compliance with the Act

The 24 agency representatives who attended our February 2003 forum acknowledged that compliance was not yet consistent across agencies and systems of records. They identified the following as the most significant barriers to improving their compliance:

- lack of sufficient OMB leadership, oversight, and guidance on the Privacy Act (first choice);
- low agency priority on implementing the act, which adversely affects the level of resources devoted to it (second choice); and
- insufficient training to satisfy the wide range of employee involvement with the act (e.g., executives have different training needs than do persons designing information systems) (third choice).

OMB Guidance and Oversight Described as Moderately Effective, but Agencies Ask for More Attention in Specific Areas

At our privacy forum, agency representatives reported that the most significant factor in uneven agency compliance was the need for additional OMB leadership on implementing the Privacy Act in today's electronic environment. Because the Privacy Act mandates that OMB provide agencies with continuing assistance and oversight, agencies look to OMB for additional help and guidance. According to agency responses to our surveys, agencies are not generally dissatisfied with OMB's guidance and assistance on the Privacy Act: for example, most agencies judged that OMB's assistance on the act was at least "moderately effective" overall. (See app. V for more detail on agency responses in this area.) However, both on the surveys and at the forum they named a number of specific areas in which they wanted further guidance, including the application of the Privacy Act to electronic records.

To address this first barrier, the most important action the agency representatives identified was that OMB should become more proactive by publishing additional guidance in certain areas and providing increased assistance to agencies. Several forum participants also noted the abundance of guidance available from the Department of Justice on the Freedom of Information Act and expressed interest in having similar information made available on the Privacy Act. Forum participants also suggested that it would be helpful if OMB were to convene periodic meetings of Privacy Act officers to discuss important areas where the guidance is not clear. Participants saw such meetings as opportunities for agencies to let OMB know where guidance and assistance were needed, to pool their knowledge, and to work with OMB to leverage resources (such as training information).

In addition, on our surveys, nine agencies reported that specific additions or revisions to OMB guidance were needed for them to better implement the act. Among the areas of the act cited most frequently were

- 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) under the act,[24] and
- cost-benefit guidance for computer matches.[25]

The observation that additional OMB guidance on the Privacy Act would be helpful is not new. In our previous reports in this area, we have recommended that OMB issue guidance on Web site privacy policies and on agencies' use of cookies.[26] Similarly, in response to the May 1998 privacy initiative, agencies requested updated guidance, particularly with regard to new technologies, and suggested that OMB establish an interagency task force and host periodic conferences on privacy. OMB has not yet acted either on our recommendations or on previous agency requests for additional guidance.

Agencies See Privacy Act Implementation as Receiving Low Priority

Forum participants reported that agency management tends to assign low priority to implementation of the Privacy Act. They commented that implementation was classed among support functions, which are often the first to be cut when resources are tight, and that Privacy Act offices were often "buried" in agencies. Also, Privacy Act officers may find themselves placed in an adversarial position when they tell their management not to take certain actions that could violate the act. Further, there was general agreement among forum participants that OMB officials had not demonstrated that the Privacy Act was a priority, and that this low priority tended to result in a similar low priority at agencies. One participant cited the minimal level of OMB resources devoted to assisting agencies to carry out the act—primarily one person—as indicative of the low priority placed

[24]According to OMB guidance, the act only covers individuals acting in a personal capacity rather than acting in a business capacity (e.g., as entrepreneurs). The guidance states "Agencies should examine the content of the records in question to determine whether the information being maintained is, in fact, personal in nature. A secondary criterion in deciding whether the subject of an agency file is, for purposes of the act, an individual, is the manner in which the information is used: i.e., is the subject dealt with in a personal or entrepreneurial role." Privacy Act Implementation: Guidelines and Responsibilities, *Federal Register*, vol. 40, no. 132 (July 9, 1975).

[25]The Computer Matching Act requires that a benefit/cost analysis be part of an agency's decision to conduct or participate in a matching program. However, the act authorizes the agency Data Integrity Boards to waive this requirement in certain circumstances.

[26]U.S. General Accounting Office, *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO/GGD-00-191 (Washington, D.C.: Sept. 5, 2000); *Internet Privacy: Implementation of Federal Guidance for Agency Use of Cookies*, GAO-01-424 (Washington, D.C.: Apr. 27, 2001).

on the act. Furthermore, participants said this lack of OMB leadership and top management attention tended to adversely affect the resources that agencies assigned to carrying out the act.

To address this second barrier, the most important action the forum participants identified was for agency top managers to place increased priority on implementing the act, including making additional resources available. However, when asked in the survey about the resources that are devoted to implementing the act, most agencies were unable to answer many of the questions. Agencies are not required to track such resources, and many respondents found estimating the resources burdensome. In appendix VI, we provide limited information on this topic, as well as on the organizational structures that agencies have set up to implement the Privacy Act.

Agencies See a Need for Increased and More Focused Training on the Privacy Act

Forum participants stated that the agencies did not provide sufficient training for agency staff who handle personal information subject to the act. They stated that the most important action to address this barrier was OMB overseeing the development of additional training for employees with varying degrees of involvement with the act and making the training more readily available (perhaps on the Web or on CD). Several participants noted that there should be role-based training that varies based on the employees' involvement with the act. For example, there could be a general orientation session on the act for all employees, and different training for executives, Privacy Act officers, and systems managers.

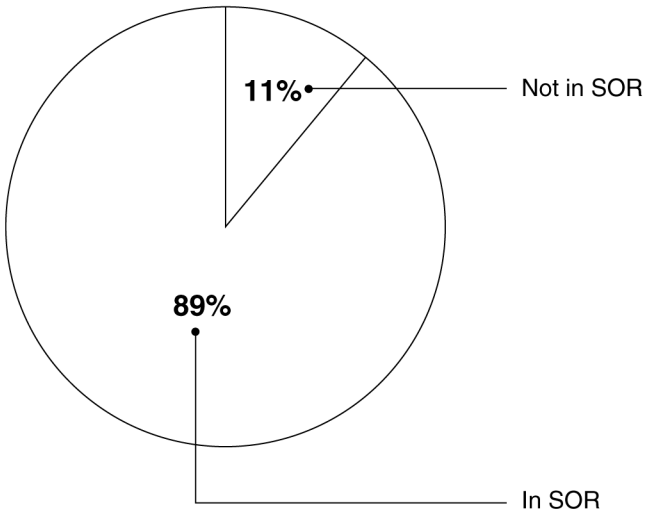
Further details on the forum results are provided in appendix II.

Agencies Maintain Personal Information outside the Privacy Act in a Limited Number of Information Systems

The protections of the Privacy Act are limited to personal information that is retrieved by a personal identifier. Over the years since the act's passage, concerns have been raised regarding the protection of personal information that does not fall within the scope of the act. (For example, electronic databases frequently permit the retrieval of personal information by search terms other than a personal identifier.) A preliminary step to addressing these concerns is to estimate the extent of personal information that is maintained outside Privacy Act systems. Based on agency responses to our survey, we estimate that 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.[27] (See fig. 10.)

Figure 4: Information Systems Containing Personal Information Not in a Privacy Act System of Records

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



Source: GAO.

[27]The 95 percent confidence interval of the estimated 11 percent is from 6 percent to 19 percent. The corresponding total estimate of 83 has a confidence interval of 44 to 139.

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

Agencies reported that they maintain personal information outside a system of records when the information

- is not retrieved by use of identifying information (e.g., name), but rather 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 these 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 stated that it 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.

However, a few agencies reported that, for administrative convenience, they put such information in Privacy Act systems of records even when not required. (OMB guidance encourages agencies to do this.) For example, the Department of Health and Human Service's Center for Disease Control maintains records on deceased individuals. These records also have information about living persons (for example, the next of kin). Therefore, all the information is maintained in a Privacy Act system of records.

Other laws besides the Privacy Act provide certain privacy and security protections to personal information outside Privacy Act systems of records. Under the Freedom of Information Act (FOIA), as amended, the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. Two exemptions in FOIA protect personal privacy interests from disclosure. The first exemption allows the federal government to withhold information

about individuals in personnel and medical files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. The second exemption allows the federal government to withhold records of information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information could reasonably be expected to constitute an unwarranted invasion of personal privacy.

A second law that protects information in federal records is the Federal Information Security Management Act (FISMA),[28] which requires federal agencies to protect agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Conclusions

Agency responses on key characteristics of their systems of records highlight the increasingly complex environment in which federal agencies must operate. Agencies reported that information is maintained on vast numbers of individuals, largely in electronic form, and that a single system of records may reside in multiple information systems. Understanding this environment—and its potential impact on individuals' privacy—will be important as the government continues to refine its privacy policies and guidance.

While Privacy Act compliance is generally high in many areas, it is not consistent across the federal government and could be improved. Agencies bear primary responsibility for compliance with the act, but they have not yet fully put into place the processes and follow-through needed to ensure compliance. Further, according to agencies, they face difficult implementation issues. Specifically, OMB has not responded either to long-standing agency requests or to our recommendations for improved guidance. In addition, agencies believe that OMB has not provided enough assistance in dealing with challenges such as the low priority generally accorded to the Privacy Act and the lack of appropriate training. Until these issues are addressed by agencies and OMB and compliance with the Privacy Act across government is improved, the government cannot adequately assure the public that all legislated individual privacy rights are being protected.

[28]Title III of the E-Gov Act (P.L. 107-347).

Agencies reported that about 11 percent of their automated systems contain personal information that is not subject to the act's protections. In view of the concerns about the scope of the Privacy Act, this information may be useful as a first step in understanding this issue in the current electronic environment. Further study is required, however, to determine what information is maintained, how it is used, and the potential effects, if any, on individual privacy rights.

Recommendations for Executive Action

To improve agency compliance with the Privacy Act, we recommend that the Director, OMB,

- direct agencies to correct the deficiencies in compliance with the Privacy Act that agencies identified in this report,
- oversee agency implementation of actions needed to correct these deficiencies, and
- monitor overall agency compliance with the act.

To address implementation issues related to compliance with the Privacy Act, we recommend that the Director

- assess the need for specific changes to OMB guidance, especially with regard to electronic records, and update the guidance, 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 recommend 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.

The Director should involve federal agencies as appropriate in addressing the above recommendations. One option for doing so would be to establish a multiagency working group or forum, perhaps as part of the Chief Information Officers Council.

Agency Comments and Our Evaluation

We provided a draft of this report to OMB for review and comment. In a letter dated June 20, 2003, the Administrators of OMB's Offices of Information and Regulatory Affairs and of E-Government and Information Technology provided comments. This letter is reprinted in appendix VII along with our additional analysis of the comments.

The Administrators stated that our report has taken an important first step toward identifying areas in which further research and discussion can be undertaken, including through a series of meetings with agency officials. However, the Administrators stated that the information presented does not support the conclusion in the draft report that without improved compliance, the government cannot assure the public that individual privacy rights are being protected. Specifically, the Administrators fault what they characterize as a fundamental flaw in the draft report: our treatment of the various provisions of the act as equally important in protecting privacy. In addition, they note that while compliance may not be perfectly consistent, a lack of perfect consistency from one agency to the next "should hardly be surprising" across the dozens of agencies that make up the government. Further, the Administrators state that the draft report does not indicate whether agency compliance with the Privacy Act is more uneven than is agency compliance with other laws, such as the Administrative Procedures Act, and so our findings on the Privacy Act do "not really say much." Finally, OMB disagrees with our recommendations, stating that they are vague and nebulous.

We disagree with OMB's overall comment that the information in the draft report does not support our conclusion. We continue to believe that without improved compliance, the government cannot adequately assure the public that all legislated individual privacy rights are being protected. In passing the Privacy Act, the Congress enacted a series of requirements designed, in total, to ensure protection of individuals' privacy. Accordingly, we believe that because agencies did not consistently comply with these

requirements, it is reasonable to conclude that the government lacks adequate assurance that privacy rights are being protected. With regard to the lack of consistency across agencies, our report does not address whether federal agencies have consistent practices, but whether federal agencies are consistently following legal requirements imposed by Congress and those practices that OMB found sufficiently important to be included in its Privacy Act guidance. Further, we believe that federal agencies should strive for consistent compliance with these requirements and others mandated by the Congress.

Regarding our recommendations, the draft report contains extensive details on agency noncompliance with specific provisions of the Privacy Act and OMB guidance. In addition, it contains many specifics on agencies' suggestions for improvements in guidance. Further, we believe our recommendations provide the appropriate level of detail needed for OMB to address the issues from a governmentwide perspective. We recognize, however, that our compliance results, in particular, are presented in aggregate form; we did not include our more detailed results in the report because this material is voluminous and because agencies are already well aware of the specific shortcomings in compliance. Nonetheless, we will be providing OMB with additional details to help in its improvement efforts.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies of this report to the Director of the Office of Management and Budget and the heads of other interested congressional committees. We are also sending copies to the 25 departments and agencies we surveyed. Copies will be made available to others on request. In addition, this report will be available at no charge on GAO's Web site at www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send E-mail to *koontzl@gao.gov*. Key contacts and major contributors to this report are listed in appendix VIII.

Sincerely yours,

Linda D. Koontz
Director, Information Management Issues

Scope and Methodology

We asked the following 25 departments and agencies to respond to survey questions about their privacy practices and procedures:

- Departments: Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, Veterans Affairs

- Agencies: Equal Employment Opportunity Commission (EEOC), Federal Emergency Management Agency (FEMA), Office of Personnel Management (OPM), National Science Foundation (NSF), Office of Government Ethics (OGE), Small Business Administration (SBA), Social Security Administration (SSA), Pension Benefit Guaranty Corporation (PBGC), Federal Trade Commission (FTC), Office of Special Counsel (OSC), Securities and Exchange Commission (SEC)

We selected these agencies to provide a cross section of large and small agencies that were likely to have different missions and organizational structures and, perhaps, different approaches to implementing the Privacy Act. In fiscal year 2002, the nine small agencies—EEOC, FEMA, OPM, NSF, OGE, PBGC, FTC, OSC, and SEC—had a median of approximately1,200 full-time equivalent staff years; the range of staff years was from 80 (OGE) to approximately 3,000 (SEC). For the remaining two large agencies and 14 departments, the median number of staff years was 64,268, with a range from approximately 4,517 (SBA) to approximately 670,166 (Defense). Each agency decided which person was best qualified to respond to the survey and who in management was to review and approve the response. We use the term "agency" to refer to (1) executive departments such as the Department of Justice and (2) independent agencies such as OPM.

Surveys

We used three surveys to obtain information on the following areas: the first addressed agencywide practices, and the second addressed systems of records; these two surveys contained questions on the characteristics of systems of records and compliance with the act and related OMB guidance. The third survey focused on information technology projects; for these, we asked questions on systems containing personal information not subject to the act's protections.

Survey on agencywide practices. We asked these 25 agencies to answer questions about agencywide Privacy Act practices and procedures (e.g., how many systems of records exist). Each agency decided which person was best qualified to respond to the survey and who in management was to

review and approve the response. In 18 of the 25 agencies, the person completing the survey was the person who had day-to-day responsibility for implementing the Privacy Act and was also the agency's Privacy Act officer. These persons were, on average, three levels removed from the head of the agency and had been performing these duties at this agency an average of 8 years. The questionnaire also contained questions about compliance with specific Privacy Act provisions and related OMB guidance. To help ensure that agencies understood the questions, we pretested the survey with agency officials. We achieved a 100 percent response rate.

Survey on systems of records. We also surveyed agencies to gather information about their systems of records' compliance with Privacy Act requirements and OMB guidance. The population for this survey consisted of all systems of records that existed in the 25 agencies as of December 1999. From this population of 3,637 systems of records, we selected a probability sample of 204. This was a stratified sample consisting of two strata. The following table summarizes the population size, sample size, and respondents by sample.

Table 3: Respondents to Second Survey

Stratum	Population	Sample size	Respondents	Response rate
Certainty	19	19	18	95%
All others	3618	185	179	97%
Total	**3637**	**204**	**197**	**97%**

Source: GAO.

The certainty sample consisted of 19 systems of records that were considered to be large or otherwise important systems for this survey. Approximately one-third of the selected systems of records no longer existed at the time of the survey. Therefore, estimates from our survey project to an estimated population of 2,443 (±244) systems of records from 1999 that still existed at the time of the survey.

Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval. This is the interval that would contain the

actual population value for 95 percent of the samples that we could have drawn. As a result, we are 95 percent confident that each of the confidence intervals in this report will include the true values in the study population. All percentage estimates in this report have 95 percent confidence intervals of ±10 percentage points or less, unless otherwise noted.

To help ensure that agencies understood the questions, we pretested the survey with agency officials. We achieved a 96 percent response rate.

Survey on information technology projects and information outside privacy act systems of records. We also surveyed agencies concerning a sample of 150 information technology projects randomly selected from 17 agencies' budget Exhibit 53s for fiscal year 2002 (Exhibit 53 is required by OMB Circular A-11).[1] We first asked agencies if these projects contained any information systems in use; if they did, we then asked questions about those information systems. We selected our sample of 150 information systems from a population of 730 that were in use in fiscal year 2002. To help ensure that agencies understood the questions, we pretested the survey with agency officials. We achieved a 76 percent response rate.

Analysis of survey results. All of our samples are probability samples and produce estimates that could vary for any particular random sample chosen. Unless otherwise noted, we are 95 percent confident that the true value is within ±10 percentage points of estimated percentages.

To minimize the chances of introducing into our results errors not related to sampling, we reviewed the agencies' responses to our surveys, asked respondents to clarify answers, validated a sample of responses, and verified a sample of the survey data keypunched into our database to ensure that it was accurate.

Based on agency responses to each of the compliance questions, we developed a compliance score for particular provisions of the Privacy Act and related OMB guidance. For example, if agencies returned 180 surveys that contained answers to a compliance question, the maximum number that could comply with the requirement would be 180. Then, if agencies

[1]The 17 agencies that had prepared budget Exhibit 53s were (1) Agriculture, (2) Commerce, (3) Defense, (4) Education, (5) Energy, (6) Health and Human Services, (7) Interior, (8) Justice, (9) Housing and Urban Development, (10) Labor, (11) State, (12) Transportation, (13) Treasury, (14) VA, (15) FEMA, (16) OPM, and (17) SSA.

reported compliance on a particular question in 140 of the 180 surveys, we would assign a score of 78 percent (140 divided by 180) to that question.

To help ensure the accuracy of answers related to compliance with the Privacy Act or OMB guidance, we randomly selected 20 percent of agencies' responses to the survey of agencywide practices and 10 percent of responses to the survey on systems of records and asked officials to provide documentation or additional narrative explanations to support their answers for key compliance questions. In addition, when agencies stated in their responses that they had issued certain public documents required under the act (e.g., a regulation), we located and reviewed the documents to be certain that they had been issued. The results of this validation work gave us greater assurance about the accuracy of agencies' survey responses. We also emailed relevant portions of the draft report to officials in the Departments of Defense, Justice, Health and Human Services, Labor, Transportation, Treasury, and officials at OGE, SEC, SBA, SSA, and OPM, that are mentioned specifically in the report**,** for their review and comment. Each of the agencies emailed suggestions to clarify particular sections of the report, which we included in this report as appropriate.

Privacy Act Forum

To better understand the implications of our survey results, we invited the 25 agencies to send a representative (mostly Privacy Act officers) to a meeting in February 2003, and 24 participated. At this meeting, we presented the survey results and then asked the participants to identify the barriers to improved compliance with the act, actions needed to improve compliance, and other issues. After participants discussed their answers to these questions, we asked them to use electronic devices to anonymously record their "votes" on various privacy issues. To identify the relative importance of the barriers to agency compliance generated by participants, we assigned different point values to the participants' first, second, and third choices. For example, we told participants their first choice for the most important barrier to improving compliance would receive three points, their choice for the second most important barrier would receive two points, etc. We also asked participants to discuss the adequacy of the act in today's electronic environment and what changes, if any, were needed to the act. We incorporated the results of these discussions and votes into the appropriate sections of this report. (See app. II for a summary of the results.)

Presidential Privacy Initiative

We reviewed the responses to the President's memorandum of May 14, 1998; OMB's memorandum of January 7, 1999; and subsequent agency reports to OMB regarding their reviews of their Privacy Act systems of records and other privacy practices. We entered the 72 executive departments and agencies' responses into a database and summarized them.

Summary of GAO's February 2003 Privacy Forum on the Survey Results

To better understand the results of our surveys, we invited the 25 agencies we surveyed to send a representative to a privacy forum at GAO headquarters in February 2003. At this forum, we presented the key results from our surveys and then asked the following questions:

- What are the major barriers to improving agency compliance with the Privacy Act?
- What actions can be taken to address these barriers?
- In view of today's electronic environment, to what extent does the Privacy Act provide adequate privacy protections to individuals?
- What changes, if any, should be made to the Privacy Act to make it more consistent with the current environment and management practices?

Twenty-four of the 25 agencies sent a representative. (The Department of Health and Human Services was not represented.) The key results from the discussion of each question are presented below.

Major Barriers to Improving Agency Compliance with the Privacy Act and Actions That Could Address These Barriers

The 24 agency representatives who attended our February 2003 forum on the survey results identified the following as the three most significant barriers to improving agency compliance:

- lack of sufficient Office of Management and Budget (OMB) leadership, oversight, and guidance on the Privacy Act (first choice, with 50 points);
- low agency priority on implementing the act, which adversely affected the level of resources devoted to it (second choice, with 36 points); and
- insufficient training to satisfy the wide range of employee involvement with the act (e.g., executives have different training needs than do persons designing information systems) (third choice, with 23 points).

Each of these barriers and the actions that could address them are discussed below.

Lack of Sufficient OMB Leadership, Guidance, and Assistance

Agency participants were in general agreement that OMB officials had not provided sufficient leadership, guidance, and assistance to agencies on the Privacy Act. Participants said that these shortcomings tended to adversely affect the resources and priorities those agencies assigned to the act.

Many representatives cited the lack of sufficient OMB guidance as a significant barrier to compliance, particularly guidance on electronic records. Among the views that participants expressed were the following:

- Agencies do not know how to fit the "paper statute" into the electronic realm in which most agencies operate today.
- OMB guidance is crucial to small agencies' successful implementation of the act, because they lack the legal resources of larger agencies.
- Lack of sufficient OMB guidance is particularly troublesome in areas where various courts have decided differently on privacy issues, and agencies need to know which legal ruling is correct.

Agency participants stated that the most important action to address this barrier was OMB demonstrating more proactive leadership by publishing additional guidance in several areas and providing increased assistance to agencies. Several participants noted the abundance of guidance available from the Department of Justice's Office of Information and Privacy on the Freedom of Information Act and wanted similar information available on the Privacy Act. It was also suggested that OMB should convene periodic meetings of Privacy Act officers to discuss important areas where the guidance is not clear. Participants saw such meetings as opportunities for agencies to let OMB know where guidance and assistance were needed, to work together by pooling their knowledge, and to work with OMB to leverage resources (such as training information). Another suggestion was that Congress provide OMB or the agencies with additional resources in the privacy area.

Low Agency Priority and Resources Devoted to the Privacy Act

Agency participants stated that agencies' top management had placed a low priority on implementing the act, and that, in turn, had adversely affected the level of resources devoted to its implementation in agencies. Participants expressed the following views:

- As a support function, Privacy Act implementation is often the first area to be cut when resources are tight. Privacy Act offices are "buried" in the agency and cannot compete with program offices, which carry out the agencies' primary missions and thus have higher priority.

- Privacy Act officers may be placed in an adversarial position when they tell their agencies not to take certain actions that could violate the act; they may need OMB to provide support for their position.

- Implementing the Privacy Act often has a lower priority than that placed on implementing the Freedom of Information Act.

- The resources that OMB devotes to assisting agencies to carry out the act suggests that OMB places less priority on the act than on its other missions; this perceived priority can affect the resources that agencies devote to it.

- In carrying out its responsibilities under the act, OMB is reactive, rather than proactive.

Participants stated that the most important action to address this barrier was for agencies (including OMB) to provide a higher priority to the act, along with the additional monetary and human resources associated with that higher priority. Several participants observed that additional resources would be made available if their agency's top managers or OMB officials placed a higher priority on implementing the act.

Insufficient Training on the Act to Meet the Wide Variety of Employee Involvement

Agency participants stated that more training was needed for agency staff that handle personal information subject to the act. This statement is consistent with the results of our survey, in which 5 of the 25 agencies reported that they had less than adequate procedures to ensure that personnel with access to systems of records are adequately trained.

In particular, forum participants noted the difficulty of communicating privacy requirements to technical staff who deal with information systems:

- Communication problems arise between Privacy Act officers and system managers regarding technology issues; privacy staff may need more technical knowledge, and technical staff may need more Privacy Act knowledge.

- Because the E-Gov Act[1] will require privacy impact assessments before information systems are built, system managers and privacy officials may have to communicate more often. However, this legislation does not affect existing databases, which currently lead to many of the communication problems.

- OMB guidance does not sufficiently communicate how to adequately protect personal information in large automated databases.

Agency participants stated that the most important action to address this barrier was OMB overseeing the development of additional training for employees who have varying kinds and degrees of involvement with the act and making the training more readily available (perhaps on the Web or on CD). Several participants noted that there should be role-based training that varies based on the employees' involvement with the act. For example, there could be a general orientation session on the act for all employees, and different training for executives, Privacy Act officers, and systems managers.

Adequacy of Privacy Act Protection in Today's Electronic Environment

Eleven of the 23 agency representatives (48 percent) who attended our February 2003 forum (one did not answer the question) believed to a "moderate" extent that in today's electronic environment, the Privacy Act provides adequate privacy protections to individuals. Among the remaining 12, no agency representative chose "very great extent"; 7 chose "great extent"; 4 chose "some extent"; and 1 chose "little or no extent."

Among the privacy issues that participants said were raised by today's electronic environment are the following:

- Electronic records are easier to collect than are paper records, perhaps resulting in some information being collected that may not be needed. (The Privacy Act states that agencies shall collect only information that is relevant and necessary.)

- Electronic records are easier to access and thus might not be protected as well as paper records. Participants raised the question of whether

[1]Public Law 107-347 (Dec. 17, 2002). Among other things, this act seeks to expand the delivery of government services through greater use of the Internet and computer resources.

electronic records should have a different level of protection under the act than paper records. (The Privacy Act states that agencies are to establish appropriate administrative, technical, and physical safeguards for personal information.).

- The aim of some E-government initiatives to increase the collection and sharing of personal information among agencies could be in conflict with the Privacy Act's goal to constrain the government's ability to use personal information.
- The ease with which electronic databases can be created and merged may result in "unofficial" systems of records; agencies may not know how their data are being used.
- The definition of "record" may need updating, along with other terms in the act, to reflect today's electronic environment.
- Homeland security needs may be generating more personal information that is maintained outside the act, raising privacy concerns.
- Insufficient attention may have been paid to agencies' collection and maintenance of personal information via the Internet and the conformance of these activities with the act's requirements.
- Guidance is not available on how to give access to electronic records that contain the names of multiple people, each of whom has rights to retrieve the same record.

Need for Changes in the Privacy Act for Consistency with the Current Environment and Management Practices

There was no general agreement among participants on desired changes to the act; rather, many participants said their concerns could be addressed through revisions to OMB guidance and were opposed to making any changes to the act. However, other participants suggested that Congress revisit several areas of the act, including the following:

- *Computer matches.* Specifically, Congress should extend the time frames for the initial computer match agreements and renewals from 18 months and 12 months to 3 years and 2 years, respectively. They believed this is needed because it would reduce the excessive burden on agencies of having to renegotiate these complex documents so frequently.

- *Disclosures pursuant to courts of competent jurisdiction under section (b)-11.* There are federal, state, local, and tribal court systems in this country. Congress needs to clarify whether requests from nonfederal courts are covered under this section.

OMB Guidance on Privacy

OMB's primary guidance to agencies on implementing the Privacy Act is *"Privacy Act Implementation, Guidelines and Responsibilities,"* 40 FR 28948 (July 9, 1975), and Appendix I to OMB Circular No. A-130, "Management of Federal Information Resources," Transmittal Memorandum No. 4 (effective Nov. 28, 2000), 65 FR 77677 (Dec. 12, 2000).

In addition, as of April 2003, OMB's Web site had links to the following memoranda and other documents categorized as "Privacy Guidance," which covered a variety of topics:

- *M-01-05, Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy* (December 20, 2000).
- *Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy* (September 5, 2000).
- *Letter from Roger Baker to John Spotila on federal agency use of Web cookies* (July 28, 2000).
- *Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act* (June 21, 2000).
- *M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000).*
- *M-99-18, Privacy Policies on Federal Web Sites* (June 2, 1999).
- *M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"* (January 7, 1999).
- *Biennial Privacy Act and Computer Matching Reports* (June 1998).
- *Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996* (November 3, 1997).

Finally, OMB's Web site had other links to "Privacy Reference Materials":

- *Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974*, 56 FR 18599 (April 23, 1991).

- *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988*, 54 FR 25818 (June 16, 1989).

- *Guidance on Privacy Act Implementations of Call Detail Programs*, 54 FR 12290 (April 20, 1987).

- *Privacy Act Guidance*—Update (May 24, 1985).

- *M-83-11, Guidelines on the Relationship Between the Privacy Act of 1974 and the Debt Collection Act of 1982*, 48 FR 15556, April 11, 1983 (March 30, 1983).

- *Implementation of the Privacy Act of 1974, Supplemental Guidance*, 40 FR 5674 (December 4, 1975).

- *Congressional Inquiries which Entail Access to Personal Information Subject to the Privacy Act* (October 3, 1975).

Compliance with Privacy Act and Associated Guidance

Table 4 shows the questions asked on our survey of agencywide practices, along with the agency responses that indicated compliance. For some questions, the maximum number of agencies that needed to answer the question is less than 25 (e.g., certain provisions of the act may not apply to all agencies).

Table 4: Responses to Agencywide Practices Survey

Compliance questions	Compliance
Does your agency account for disclosures of personal information outside of your agency? (Q.3)	25 of 25
Has your agency issued a *Federal Register* notice explaining the reasons for exemption? (Q12)	24 of 24
Under the Privacy Act, does your agency have a Data Integrity Board? (Q35) [a]	13 of 13
Has your agency established rules in the Code of Federal Regulations for determining if the individual is the subject of a record? (Q.1.1)	24 of 25
Has your agency established rules in the Code of Federal Regulations for handling requests for access to records? (Q.1.2)	24 of 25
Has your agency established rules in the Code of Federal Regulations for amending records? (Q1.3)	24 of 25
Has your agency established rules in the Code of Federal Regulations for fees for copying records? (Q1.4)	24 of 25
Since October 1, 1998, has any court ruled that your agency violated any provision of the Privacy Act or found an employee criminally liable under the act? (Q16)	22 of 25
During fiscal years 1998–2001, did your agency review the routine use disclosures associated with each system of records to ensure that uses were compatible with the original purpose? (Q10)	21 of 25
Does your agency have procedures to ensure personnel with access to systems of records or who are engaged in developing procedures are adequately trained? (Q.5)	20 of 25
Before [new] systems become operational, does your agency have written policies or procedures for determining whether that personal information is needed?	17 of 25
During fiscal years 1998–2001, did your agency review each system of records containing exemptions to determine whether such exemptions were still needed? (Q.13)	19 of 24
During calendar year 2001, did your agency review each ongoing matching program to help ensure the requirements of the Privacy Act and OMB guidance have been met? (Q.33)	9 of 13
Has your agency established rules of conduct for persons who are involved in operations and maintenance of records? (Q.2.2)	16 of 24
Has your agency established rules of conduct for persons involved in design and development of systems of records? (Q.2.1)	15 of 24
During fiscal year 2001, did your agency review each system of records' *Federal Register* notice to ensure that it accurately described the system of records? (Q.8)	15 of 25

Source: GAO analysis of survey data.

[a]There are other compliance questions that ask about agencies' Data Integrity Boards, but the questions are open ended, and the answers cannot be given a compliance rating.

Table 5 shows the questions asked on our survey of agencies' systems of records along with the calculated compliance scores.[1] For questions that ask "how" an agency does something, we calculated compliance scores based on their responses to the multiple choice answers embedded in the question. We have included the multiple choice responses in parentheses following those questions.

Table 5: Responses to System of Records Survey

Compliance questions	Compliance
Since October 1, 2000, did any persons, without authorization, read, alter, disclose, or destroy any personal information in the information system? (Q.17)	100 percent
Has your agency promulgated a final rule under the Administrative Procedure Act that explains why your agency considers the exemption necessary? (Q.55)	100 percent
Has any court ruled that your agency violated any provision of the Privacy Act or found an employee criminally liable regarding this system of records? (Q.48) [a]	100 percent
How does your agency ensure the personal information that is used in making a determination about an individual is complete, accurate, relevant and timely? (do not ensure completeness, accuracy, relevance and timeliness of the information; verify with other records within the agency; verify with other federal agencies' records; verify with subject individuals; verify with state and local agencies; verify with private-sector records (e.g., banks, former employer); system of records is exempt from this requirement; no actions are taken; other (please specify); information is not used in making a determination) (Q.36)	95 percent
Is there a plan for the security and privacy of the automated information system? (Q.12)	94 percent
Are there disposition schedules for the records in this system of records? (Q.49)	91 percent
Has your agency issued a *Federal Register* notice containing the following information for this system of records? (name and location of the system of records; categories of individuals covered; routine uses that apply; policies and procedures to store, retrieve, retain, and dispose of records; how individuals can find out if the system contains a record pertaining to them, ask for access to any records pertaining to them, or contest the accuracy of any records pertaining to them) (Q.2)	89 percent
Would your agency be able to account for all disclosures of individuals' records to organizations or individuals outside your agency? (Q.42)	86 percent
During fiscal years 2000 or 2001, did your agency review the performance of [a contractor operating a system of records on behalf of the agency] to help ensure that it was complying with the Privacy Act? (Q.31) [b]	85 percent
During fiscal years 1998–2001, did your agency review the exemptions to determine whether these exemptions were still needed? (Q.54) [b]	85 percent
During fiscal years 1999–2001, did your agency assess the threats, vulnerabilities, and effectiveness of current or proposed safeguards? (Q.13)	82 percent

[1]For some compliance questions, a sufficient number of agencies did not respond at a rate that allows us to be 95 percent confident that the true value is within ±10 percentage points of estimated percentages. Unless otherwise noted, we deleted those questions from our analysis and from the table.

(Continued From Previous Page)

Compliance questions	Compliance
For individuals who are asked to supply personal information, does your agency inform them, in writing, of the authority for requesting the information, how the information may be used, whether providing the information is mandatory or voluntary, and the consequences of not providing the information? (Q.35)	82 percent
During fiscal years 1998–2001, did your agency review the routine use disclosures to ensure they continue to be compatible with the purpose they were collected for? (Q.37)	82 percent
During fiscal year 2000 or 2001, did your agency review the *Federal Register* notice to ensure that it was accurate? (Q.4)	79 percent
Before disclosing records to a nonfederal organization, how does your agency ensure that the information in this system is complete, accurate, relevant, and timely? (do not ensure completeness, accuracy, relevance and timeliness of the information; verify with other records within the agency; verify with other federal agencies' records; verify with subject individuals; verify with state and local agencies; comparison with private-sector records (e.g., banks, former employer); system of records is exempt from this requirement; no actions are taken; other (please specify) (Q.40) [b]	71 percent

Source: GAO analysis of survey data.

[a]Agencies reported two systems of records where there were court rulings that the agency violated the Privacy Act. However, the table indicates 100 percent compliance because these two systems of records were not in our random sample and thus not weighted sufficiently to lower compliance below 100 percent.

[b]Confidence interval of ±15 percent.

Agency Views on OMB Guidance and Assistance

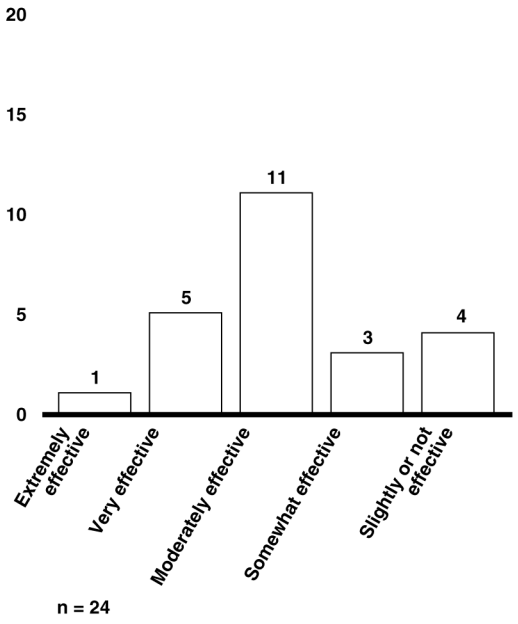
On our survey, agencies responded to a series of questions regarding OMB's guidance and assistance to agencies, with most ratings falling in the middle range.

OMB's Overall Assistance to Agencies Was Frequently Judged "Moderately Effective"

Of 24 agencies responding,[1]11 reported that, overall, OMB's assistance on the act was "moderately effective"—that is, a "3" on a 5-point scale. Figure 5 shows the breakdown of responses.

Figure 5: Agency Characterization of Overall Effectiveness of OMB Assistance

In providing assistance on Privacy Act issues in your agency, overall, how would you characterize OMB's effectiveness?



Source: GAO.

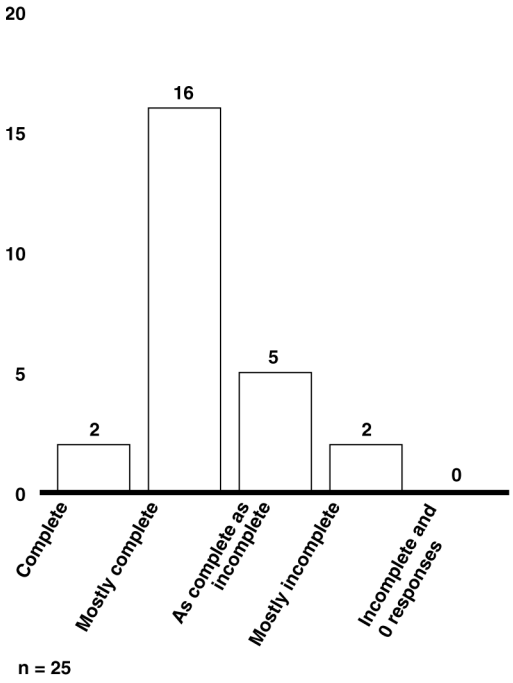
[1]One agency did not respond to this question.

OMB's Written Guidance Was Frequently Judged "Mostly Complete"

Sixteen agencies stated OMB's written guidance was "mostly complete"—a "2" on a 5-point scale. Of the remaining nine agencies, seven assessed OMB's guidance lower (3 or 4), and two rated it higher as shown in the figure below. For example, one agency reported it was "mostly incomplete" and stated "Guidance [is needed] on safeguarding the security of electronic records and the application of the Privacy Act to electronic records." None rated it as "incomplete." In contrast, another agency reported the guidance was "mostly complete" and stated it was "very useful, especially the 1975 PA guidelines and the 1989 guidance on computer matching."

Figure 6: Agency Characterization of Completeness of OMB's Written Guidance

How would your agency characterize the completeness of OMB's existing written guidance to agencies for the Privacy Act?



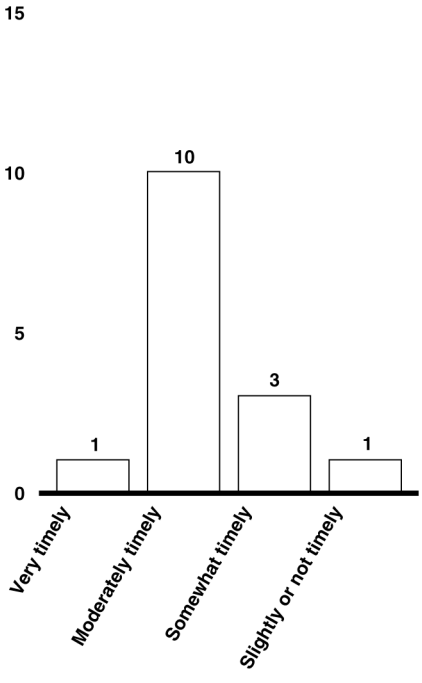
Source: GAO.

OMB's Responses to Agency Questions Were Frequently Judged "Moderately Timely"

Ten of the 15 agencies that rated OMB's timeliness in responding to agency questions about the act chose "moderately timely" a "2" on a 4-point scale. Of the remaining 5 agencies, 4 assessed OMB's timeliness lower (3 or 4), and 1 rated it higher (1), as shown in figure 7. In comments regarding this issue, an agency official stated, "In general, greater emphasis needs to be placed on the Privacy Act by OMB. In particular, additional human resources should be devoted to fulfill OMB's responsibilities under subsection (v) of the Act, additional written guidance is needed, and oral guidance should be more readily accessible and obtainable."

Figure 7: Agency Characterization of Timeliness of OMB's Response to Questions

Overall, during fiscal years 2000 and 2001, how would your agency characterize the timeliness of OMB's response to your questions related to the Privacy Act?



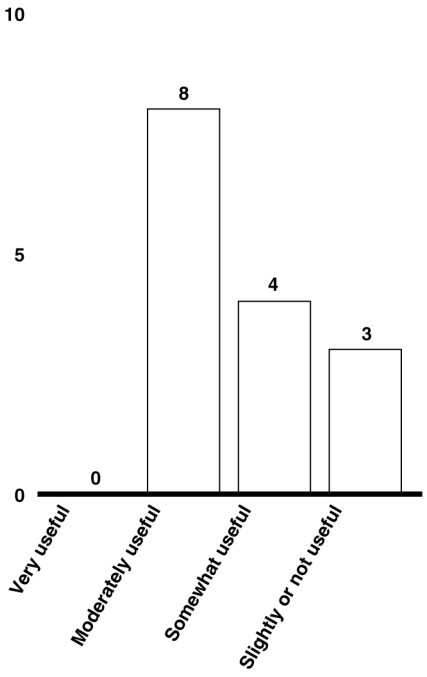
Source: GAO.

With regard to the *usefulness* of OMB's responses to agency questions about the Privacy Act, 8 of 15 answering the question reported that OMB's

responses were "moderately useful"—a "2" on a 4-point scale, as shown in figure 8.

Figure 8: Agency Characterization of Usefulness of OMB's Response to Questions

Overall, during fiscal years 2000 and 2001, how would you characterize the usefulness of OMB's response to your agency's questions related to the Privacy Act?



Source: GAO.

OMB's Assistance on Agencies' *Federal Register* Notices Was Frequently Judged "Moderately Timely"

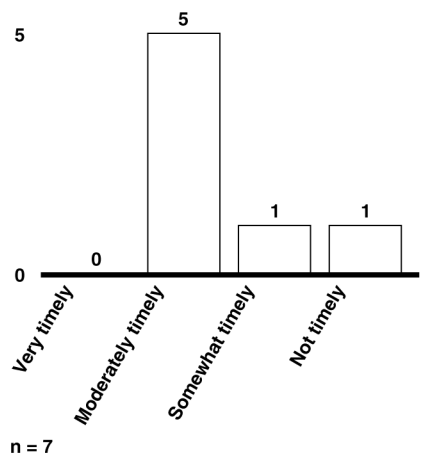
Under the Privacy Act, agencies' *Federal Register* notices for systems of records are to contain the name and location of the system of records, the routine uses of the personal information in the system, the categories of persons covered, and procedures for persons to ask for access to any records pertaining to them.

We asked about the timeliness of OMB's assistance in writing *Federal Register* notices. Most agencies (18 of 25) did not ask for OMB assistance and thus did not answer the question. Among the 7 that did answer the

question, 5 agencies reported that OMB's assistance was "moderately timely"—a "2" on the 4-point scale. (See fig. 9.)

Figure 9: Agency Characterization of Timeliness of OMB's Assistance with *Federal Register* Notices

For fiscal years 2000 and 2001, overall, how would your agency characterize OMB's timeliness in responding to your request for assistance on these *Federal Register* notices?

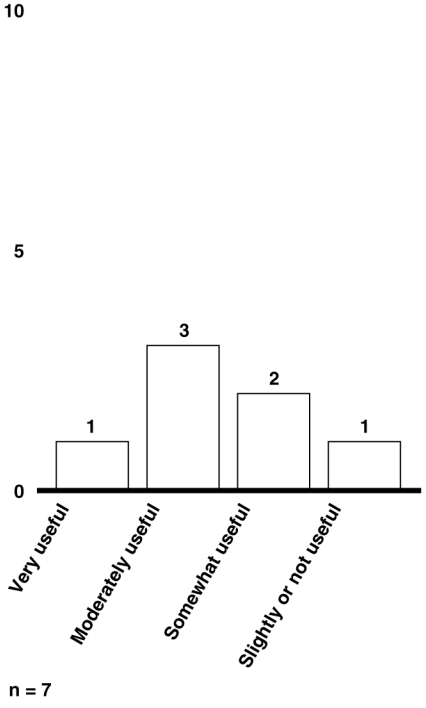


Source: GAO.

We also asked agencies to assess the usefulness of OMB's assistance in writing *Federal Register* notices using a 4-point extent scale, where "1" was "very useful" and "4" was "slightly or not useful." Among those seven agencies that answered the question, three reported that OMB's assistance was "moderately useful." (See fig. 10.)

Figure 10: Agency Characterization of Usefulness of OMB's Assistance with *Federal Register* Notices

Overall, during fiscal years 2000 and 2001, how would you characterize the usefulness of OMB's response to your request for assistance on these *Federal Register* notices?



Source: GAO.

Agency Resources and Structure Devoted to Implementation of the Privacy Act

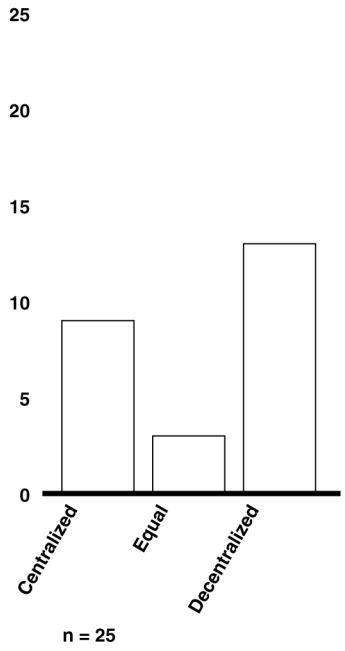
In response to our survey questions aimed at determining agency resources devoted to implementation of the Privacy Act, most agencies were unable to answer many of the questions. Of 25 agencies responding, 7 were able to report the number of employees in their agency who would spend half or more of their time on implementation of the act. They ranged from 3 employees each at the Department of Defense and the Office of Personnel Management (OPM) to 28 employees at the Department of Health and Human Services. Among the remaining 18 agencies, 10 reported that no employees would spend half or more of their time on implementation, and 8 agencies reported that they "do not know" how many employees in their agency would spend half or more of their time on implementation of the act.

Five agencies were able to report the number of full-time equivalent (FTE) staff years spent on Privacy Act implementation. The remaining 20 agencies said it was "too difficult to estimate" how many FTE staff years they will spend on the act's implementation.

We also inquired about agencies' structures for implementing the act. More than half the agencies reported having a decentralized structure to implement their Privacy Act systems of records. (See fig. 11.) "Decentralized" was defined in the survey as "Most actions under the Privacy Act are implemented at the component, bureau, or field office level." "Centralized" was defined as "Most actions under the Privacy Act are implemented at headquarters (HQ)."

Figure 11: Centralization of Implementation of Privacy Act

Consider the organizational structure for implementing the Privacy Act in your agency. Which of the following describes the way your agency is organized?



Source: GAO.

The person responsible for implementing the Privacy Act was located in the office of the Chief Information Officer (CIO) at seven agencies, the General Counsel at three agencies, and Public Affairs at two agencies; the remainder were in other offices. One agency suggested that for agencies to better implement the act, "Have all Privacy Officers report to CIOs in their bureaus." Under the Paperwork Reduction Act (44 U.S.C. 3506 (a) and (g)), the agency CIO is required to be responsible for carrying out responsibilities for compliance with the Privacy Act.

Comments from the Office of Management and Budget

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 20, 2003

Mr. Joel Willemssen
Managing Director
Information Technology Team
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for this opportunity to comment on the draft GAO report on Executive Branch compliance with the Privacy Act ("Privacy Act: OMB Leadership Needed to Improve Agency Compliance").

The Office of Management and Budget (OMB) welcomes GAO's review of Executive Branch compliance with the Privacy Act. We believe that GAO has taken an important first step in this review through the survey/questionnaire that GAO sent to a number of agencies as well as the follow-up forum that GAO held with agency representatives to discuss their survey answers. The information that GAO has received through the survey and forum will be useful in identifying areas in which further research and discussion, of a more factual and specific nature, can be undertaken. In fact, OMB plans on using the survey/forum information in this manner, as the basis for a series of meetings that OMB will convene with agencies to discuss the Privacy Act.

See comment 1.

However, as we explain below, we believe that the information which GAO has collected to date is inadequate to support the draft report's broad conclusions and recommendations. Relying on the survey/forum information, the draft report claims that there is "uneven compliance" by agencies with the Privacy Act's requirements (p.12) and that "until . . . compliance with the Privacy Act across government is improved, the government cannot assure the public that individual privacy rights are being protected" (p.26). See also the "What GAO Found" cover page: "As a result of this uneven compliance, the government cannot assure that individual privacy rights are being protected." With all due respect, these statements border on the reckless and irresponsible.

While it may be true that Privacy Act compliance is not perfectly consistent within the Federal Government, a lack of perfect consistency from one agency to the next should hardly be surprising when one considers that the Federal Government is composed of dozens of agencies. In addition, the draft report does not indicate whether Federal agency compliance with the Privacy Act is any more "uneven" than is agency compliance with other government-wide statutes such as the Administrative Procedure Act. Thus, pointing out that there is "uneven" compliance does not really say much.

The far more important question is to what extent Federal agencies are, in fact, protecting the personal information that is contained in Privacy Act records. This is a very serious question, which deserves a very serious inquiry. The draft report purports to answer this question by strongly suggesting – in a backhanded way – that there are fundamental problems with Privacy Act compliance that imperil the privacy of personal information. How else is the reader to understand the draft report when it states (at p.26) that Federal agencies and OMB must implement the draft report's recommendations (so that "compliance with the Privacy Act across government is improved") or else the Federal Government will not be able "to assure the public that individual privacy rights are being protected"? This is a very strong claim to make, and such a claim should be based on hard evidence, or at least on a set of facts that can withstand scrutiny.

The fundamental flaws in the draft report's logic become readily apparent through a careful reading of the survey/forum results and by recognizing the inherent limitations in GAO's reliance on the survey/forum for collecting information. With respect to the survey/forum results, the draft report understates the extent of the Federal Government's protection of privacy, and overstates the claim of "uneven compliance," by making the mistake of "mixing apples and oranges" – specifically, of treating the various provisions of the Privacy Act as if they are all equally important in terms of the ultimate goal of protecting privacy. In this regard, we think that one of the most important findings in the draft report is that Federal agencies reported 100% compliance with the Privacy Act's prohibition against unauthorized disclosures of information. See draft GAO report, Appendix IV, Table 5 (p. 43) (Q.17 -- agencies reported 100% compliance when asked "Since October 1, 2000, did any persons, without authorization, read, alter, disclose, or destroy any personal information in the information system?") The prohibition on disclosures, which is found in subsection (b) of the Act, is one of the Act's cornerstones.

See comment 2.

Because the Privacy Act's disclosure prohibition is a central component of the Act's overall framework for protecting privacy, we think that this 100%-compliance response should be given significant weight in evaluating the Federal Government's protection of privacy. However, this 100%-compliance figure is found nowhere in the main body of the draft report. Instead, it is mentioned only once in the whole report, in Appendix IV, Table 5. It is unclear why this figure has been buried in the appendices. (Similarly, it is unclear why, when three survey questions elicited a 100% compliance response, GAO chose to discuss in the main body of the report – as an example of a 100% response – the question that had the least immediate connection to protecting personal privacy.[1]) Does the draft report's treatment of the 100% compliance figure for the disclosure prohibition reflect a GAO belief that the Privacy Act's disclosure prohibition is unimportant, or does it instead reflect how information is treated in a draft report when it "does not fit" with the report's conclusions and recommendations? In any

[1] In the main report, GAO discussed the 100% compliance figure for the question "Has you agency promulgated a final rule under the Administrative Procedure Act that explains why your agency considers the exemption necessary?" See the "What GAO Found" cover page, and pp. 3 and 12 of the main report; see also Appendix IV, Table 5 Q.55. The third question with a 100% compliance response was "Has any court ruled that your agency violated any provision of the Privacy Act or found an employee criminally liable regarding this system of records?" See Appendix IV, Table 5, Q.48. This question, like the disclosure-prohibition question, is mentioned only in Appendix IV, and not in the main body of the report.

2

event, the draft report gives no more significance to the 100% compliance with the Act's disclosure-prohibition than it gives to the 79% compliance with the question – "During fiscal year 2000 or 2001, did your agency review the *Federal Register* notice to ensure that it was accurate?" See draft GAO report, Appendix IV, Table 5 (p. 43) (Q.4). It should be noted that this question does not ask whether agencies believe that their *Federal Register* notices are accurate, but only whether the agencies reviewed the notices for accuracy in fiscal years 2000 or 2001. We think that, in any fair evaluation of the Federal Government's protection of privacy, the level of agency compliance with the Act's disclosure prohibition must be considered as far more important than whether agencies reviewed their *Federal Register* notices in a specific two-year period.

There are several other reasons for having serious doubts about the significance of the survey/forum results, and how much weight should be placed on them. First, there is at least one internal inconsistency within the responses, and it pertains to a survey result that is discussed in the main body of the report. In the "What GAO Found" cover page at the beginning, the draft report refers to 86% of agencies being in compliance, and 14% not in compliance, with "being able to account for all disclosures of individual's records outside the agency." These results, which are also reported in Table 5 of Appendix IV (Q.42), do not seem to be consistent with the positive response of "25 of 25" agencies to the separate question "Does your agency account for disclosures of personal information outside of your agency?" Appendix IV, Table 4 (Q.3). It is not clear from the draft report how these results can be reconciled.

See comment 3.

Another problem with the survey responses involves those GAO questions that asked "how" an agency does something. The lowest percentage response in Table 5 is to a "how" question, namely, the 71% response to the question – "Before disclosing records to a nonfederal organization, how does your agency ensure that the information in this system is complete, accurate, relevant, and timely?" (Q.40). Since "how" questions do not elicit a yes-or-no answer, the draft report explains that "For questions that ask 'how' an agency does something, we calculated the compliance score based on their responses to the multiple choice answers embedded in the question." See Appendix IV, p.43. The draft report does not provide a further explanation of how GAO "calculated the compliance score," and the draft report does not enclose the multiple choice answers. In other words, the draft report leaves the reader with no choice but to accept the 71% figure. There is additional reason to doubt this 71% figure, which is that Table 5 has a 95% "compliance score" for the agencies' responses to the related question -- "How does your agency ensure the personal information that is used in making a determination about an individual is complete, accurate, relevant and timely?" (Appendix IV, Table 5, Q.36). Both questions address the issue of whether agencies maintain information in a "complete, accurate, relevant, and timely" manner, but they result in GAO-calculated compliance scores of 71% and 95%.

See comment 4.

Another reason to have concerns about the "compliance" ratings in Tables 4 and 5 is that many of the questions that had the lowest ratings were framed in a very narrow manner, which asked whether each agency had undertaken a particular activity in a specific fiscal or calendar year. For example, in Table 4, "15 of 25" agencies answered

See comment 5.

"yes" to the question (Q.8) -- "During fiscal year 2001, did your agency review each system of records' *Federal Register* notice to ensure that it accurately described the system of records?" Another example is that "20 of 25" agencies answered "yes" to the question (Q.4) – "During fiscal year 2001, did your agency review training practices to ensure personnel are familiar with the Privacy Act and other special requirements of their specific job." Another example is that "9 of 13" agencies answered "yes" to the question (Q.33) – "During calendar year 2001, did your agency review each ongoing matching program to help ensure the requirements of the Privacy Act and OMB guidance have been met."

See comment 6.

It is not clear what conclusions, if any, should be drawn from the fact that 5 of 25 agencies said that they did not review their training practices in FY01. After all, it is entirely possible that those 5 agencies reviewed their training practices in the year before (FY00) and/or the year after (FY02). In any event, whether or not the 5 agencies reviewed their training practices – in any of those years – is a different question from whether their training practices are in fact appropriate and effective. What does it mean if an agency did not review its training practices in FY01, but those practices – if they had been reviewed – would have been found to be appropriate and effective? The same is true for the other two "review" questions noted above. In the absence of additional information, these questions and answers do not say much, if anything. And, these answers certainly do not support the draft report's broad claim that, "[a]s a result of this uneven compliance, the government cannot assure that individual privacy rights are being protected." These "review" questions and answers, which do not appear to be meaningful in isolation, do not somehow gain meaning when they are juxtaposed with other questions and answers that do have meaning, such as the 100% figure for agency compliance with the Privacy Act's disclosure prohibition. To repeat the point made earlier above, the draft report inappropriately "mixes apples and oranges" by treating every question and answer as equally significant and meaningful.

See comment 7.

The final fundamental flaw with the factual underpinnings of the draft report is the extremely limited nature and scope of the facts that GAO has actually reviewed. By relying so heavily on the results from its survey and forum, the draft report has fallen into "the numbers trap" of confusing the data that you happen to have at your fingertips with the data that is actually relevant and meaningful for evaluating an issue. The survey and forum results comprise virtually all the information that the draft report relies upon for its broad conclusions and recommendations. Two other pieces of information in the report, which are given only cursory references, are the prior reports that GAO has issued on OMB's website privacy policy and on computer security (p.8 and fn.13-15); neither of these issues directly involve the Privacy Act. There is also a reference in the draft report to a 1983 House Committee oversight report on the Privacy Act (p.9 and fn.10); naturally, this 1983 report does not have information about the Federal Government's efforts for the past 20 years. Thus, in the final analysis, there is no factual material in the draft report except for the survey and forum results.

It is important, therefore, to recognize all the kinds of factual information about the Privacy Act that are not found in the draft report. As an initial matter, it is significant

See comment 8.

See comment 9.

See comment 10.

that the draft report does not point to even a single report issued by GAO or by an Inspector General (OIG) that evaluates and finds deficiencies with any agency's compliance with the Privacy Act. This is quite remarkable. GAO and the OIGs issue reports on a daily basis in which they investigate and scrutinize Federal agencies' compliance with a wide range of their statutory responsibilities. The absence of any GAO and OIG reports on Federal agency compliance with the Privacy Act means either that (1) such reports have been issued, but GAO did not look for them, (2) such reports have not been prepared, and that is because GAO and OIGs do not consider agency compliance with the Privacy Act to be important, or (3) such reports have not been prepared, and that is because agency compliance with the Privacy Act has generally been viewed as being relatively high, and thus has not warranted GAO or OIG review. In any event, it is significant that the draft report does not point to any GAO or OIG (or congressional) reports that identify deficiencies with the Privacy Act compliance at any particular agency or program. For how many other statutes that impose government-wide requirements can that be said? The absence of any such GAO, OIG, or congressional reports undercuts the draft report's claim that, if its recommendations are not adopted, "the government cannot assure that individual privacy rights are being protected."

Similarly, the draft report does not discuss even one of the hundreds of Privacy Act decisions that Federal courts have issued during the past three decades. As these cases make clear, individuals have the right to seek judicial review of the agencies' compliance with the Privacy Act. It would not have been difficult to review the court cases, as a way of evaluating the extent to which Federal agencies are complying with their statutory responsibilities. The wide variety of legal research materials that are available (both in paper and via computer) make it easy to review the Privacy Act case law.

The Justice Department had already carried out extensive research, which is contained in the 180-page Privacy Act Overview that the Department publishes and makes publicly available on-line, at http://www.usdoj.gov/04foia/04_7_1.html. An obvious starting point for GAO would have been the Privacy Act Overview. Thus, it is remarkable that the draft report does not mention a single court case involving the Privacy Act. As with the absence of any GAO/OIG/congressional reports on specific agency or program compliance, the absence of any discussion of the court cases undercuts the draft report's claim that, if its recommendations are not adopted, "the government cannot assure that individual privacy rights are being protected."

In addition, the draft report makes no attempt to conduct an actual review of any agency's or program's compliance with the Privacy Act. One searches in vain through the draft report for the mention of any specific agency, or any specific program, or any specific system of records that is out of compliance with any of the Privacy Act's requirements. Such facts, which one would think are crucial for an evaluation of the Federal Government's success in implementing the Privacy Act, are nowhere to be found in the draft report. Again, the absence of any such facts undermines the draft report's claim that, if its recommendations are not adopted, "the government cannot assure that individual privacy rights are being protected."

5

See comment 11.

Finally, the draft report does not even seek to reconcile the survey/forum results with one of the few real-world facts that are mentioned in the report. As the draft report notes, the OMB Director on January 7, 1999, issued a memorandum that directed the heads of all Federal departments and agencies to conduct a review of their systems of records and information holdings in order to ensure that they were in compliance with the Privacy Act. (OMB Memorandum M-99-05, which is available on OMB's website, at http://www.whitehouse.gov/omb/memoranda/m99-05.html.) This review directed each Federal agency to take the following actions, and the memorandum required senior agency officials to certify to OMB that the agency had done so:

- "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." (Attachment B, p.2)
- "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 safeguards in place are appropriate to the types of records and the level of security required." (p.3)
- "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." (p.3)
- "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." (p.4)
- "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." (p.5)
- "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

6

notices to ensure that they are up-to-date, to conform with any necessary changes identified during the review [above]." (p.5)

- "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." (p.6)

The draft report acknowledges that OMB directed the agencies to undertake this comprehensive Privacy Act compliance exercise, and the draft report notes in passing that 72 agencies submitted responses to OMB in which – in the words of the draft report (p.9) – the agencies "(1) added 131 systems of records that previously had not been properly identified, (2) revised 457 systems of records that were not up to date, and (3) deleted 288 systems of records that were no longer necessary."

However, the draft report makes absolutely no attempt to reconcile the responses to its survey/forum with the actions that agencies undertook in compliance with this comprehensive OMB-directed review of the agencies' compliance with the Privacy Act. For example, as noted above, OMB directed each agency in Fiscal Year 1999 to "review its systems of records to ensure that safeguards in place are appropriate to the types of records and the level of security required," and agencies certified to OMB that they conducted this review. However, according to Table 5 of the draft report, only 82% of the agencies answered "yes" to the survey question (Q.13) – "During fiscal years 1999-2001, did your agency assess the threats, vulnerabilities, and effectiveness of current or proposed safeguards?" GAO makes no effort to reconcile these facts.

Similarly, as noted above, OMB directed each agency in FY99 to "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," and agencies certified to OMB that they conducted this review. However, according to Table 5, only 82% of the agencies answered "yes" to the survey question (Q.37) – "During fiscal years 1998-2001, did your agency review the routine use disclosures to ensure they continued to be compatible with the purposes they were collected for?" GAO makes no effort to reconcile these facts.

In a similar vein, as noted above, OMB directed each agency in FY99 to "conduct a review of its systems of records notices to ensure that they are up-to-date," and agencies certified to OMB that they conducted this review. According to Table 5, only 79% of the agencies answered "yes" to the survey question (Q.4) – "During fiscal year 2000 or 2001, did your agency review the *Federal Register* notice to ensure that it was accurate?"

7

These facts are not inconsistent, because the OMB review occurred in FY99, and the GAO question focused on FY00 and FY01. However, how significant is the 79% rate of conducting a notice review in FY00 and FY01 when all the agencies had been directed to conduct a notice review in the prior year (FY99)? GAO makes no effort to evaluate the significance of this compliance rate.

In sum, by relying entirely on the results from its survey and forum, GAO has not taken into consideration, or even acknowledged in the report, all the other factual material that is relevant to and necessary for carrying out a serious evaluation of the Federal Government's implementation of the Privacy Act. Moreover, for the reasons discussed above, the survey/forum results are fundamentally flawed, both when considered in isolation and when considered in a broader factual context. As a result, we believe that the draft report's conclusion – namely, that, if its recommendations are not adopted, "the government cannot assure that individual privacy rights are being protected" – lacks a solid factual foundation and therefore borders on the reckless and irresponsible.

Having spent so much time addressing the report's factual analysis and conclusions, we will spend only a brief moment addressing the report's draft recommendations. As the title of the draft report indicates, GAO staff believe that "OMB Leadership" is "Needed to Improve Agency Compliance" with the Privacy Act. Since, for the reasons above, it is not clear that there is a problem with agency compliance (as opposed to GAO's review methodology), it is not clear what actions OMB should take to "improve agency compliance." The recommendations themselves are extremely vague in this regard, perhaps owing to the draft report's failure to pinpoint any real-world compliance problems. The draft report does not point to any specific "deficiencies in compliance" with reference to any particular agencies or programs (in this regard, the agencies' responses, for what they are worth, have been withheld from OMB). Thus, it is difficult to understand how OMB is supposed to "direct agencies to correct the deficiencies in compliance" or "oversee agency implementation of actions needed to correct these deficiencies" (p.27).

See comment 12.

The other recommendations are equally nebulous. For example, the draft report recommends that OMB "assess the need for specific changes to OMB guidance" (p.27), even though the draft report does not actually identify a single deficiency in any of the Privacy Act guidance that OMB has issued, or that the Justice Department has provided in its Privacy Act Overview, or that the courts have provided in their decisions.[2] In this regard, while the draft report notes that some agencies had complaints about the adequacy of OMB's written guidance, most agencies found it "mostly complete".[3] (Appendix V, Figure 6, p. 46) Again, the draft report makes no attempt to reconcile these contrary

[2] We have enclosed two complete sets of copies of the Privacy Act guidance that OMB has issued, as well as two complete copies of the Justice Departments' Privacy Act Overview. We request that GAO include a complete copy of the OMB and DOJ guidance in GAO's response to the congressional requester.

[3] In fact, based on materials that GAO prepared last fall, one of the agencies that considered OMB's guidance to be "very useful" and "mostly complete" was the Defense Department, which had nearly one-half (1,156) of the 2,443 systems of records in GAO's survey (Draft Briefing Slides, 10/08/02, pp. 29, 45).

8

views regarding the guidance. The fact that different agencies could view OMB's guidance in sharply different ways argues against drawing any firm conclusions from the survey/forum results in the absence of additional information.

Our final comment concerns GAO's interactions with OMB during GAO's collection of information and preparation of the draft report. GAO routinely asks OMB to provide GAO with information, including through interviews, on a wide range of topics, many of which do not directly relate to OMB but instead are really a review of another agency's activities. During the past year, OMB has responded to dozens of GAO inquiries. Some of them, concerning such OMB activities as the Paperwork Reduction Act, Regulatory Review, E-Government initiatives, and the Program Assessment Rating Tool (PART) have involved in-depth GAO reviews of OMB's activities. In all those cases, GAO initiated a formal review with OMB and requested the opportunity to interview OMB staff.

See comment 13.

GAO's conduct in conducting this Privacy Act review was very different, and in fact was unprecedented in our experience. During the many months of its preparation of this draft report, GAO never initiated a formal review with OMB and never requested the opportunity to interview OMB staff. In other words, it appears to us that GAO staff made no serious attempt to obtain OMB's perspective on agency compliance with the Privacy Act and on the adequacy of OMB's guidance to agencies. GAO did provide OMB the opportunity to comment on draft materials, such as this draft report and last fall's draft briefing slides, but providing us with an opportunity to comment on materials that GAO has already prepared is far different than requesting information from us to incorporate into GAO's review. OMB staff raised on several occasions the concerns that are outlined above, and they repeatedly pointed out to GAO staff that the scope of its factual review was too narrow and that GAO needed to follow-up the survey and forum results by collecting further information. OMB staff invited GAO to conduct a review of OMB's activities, during which OMB could address the concerns that agencies had raised in the survey/forum about OMB's guidance. GAO declined this invitation to conduct a review of OMB's activities, and GAO staff did not pursue the concerns and issues that OMB raised. OMB has also informed GAO staff of our more recent work in privacy, including the reinstatement of an interagency Privacy Committee, and OMB's process of drafting guidance to agencies on implementation of section 208 of the E-government Act of 2002. OMB also recently held an open forum on privacy, where GAO staff were present, and two agencies publicly praised OMB's leadership in the area of privacy.

In closing, we want to reaffirm that OMB takes seriously its responsibilities to provide guidance to the agencies and oversee their implementation of the Privacy Act. We would welcome a careful and thoughtful GAO report that identifies real-world problems with agency compliance in particular agencies and programs (or that identified

specific problems with OMB's guidance) and that provides concrete recommendations for how OMB and/or the agencies could correct these problems. However, the draft report does not provide that careful and thoughtful analysis. As noted at the beginning, we will be convening a series of meetings with the agencies to follow-up on the issues that they raised in the survey/forum results.

Thank you again for this opportunity to comment on the draft report.

Sincerely,

Mark Forman
Administrator
Office of E-Government and Information Technology

John D. Graham, Ph.D.
Administrator
Office of Information and Regulatory Affairs

Enclosures

10

GAO Comments

1. We disagree with OMB that the statements made in our report "border on the reckless and irresponsible." Our survey results represent 25 departments' and agencies' compliance with a broad range of Privacy Act provisions. These 25 cover a broad cross section of small, medium, and large departments and agencies. In most cases, agencies' Privacy Act officers—who had an average of 8 years of experience in that position—responded to our survey of agencywide practices; we achieved a 100 percent response rate on this survey. Our survey concerning a sample representing a population of 2,400 systems of record was completed by the person the agency deemed as most knowledgeable of that system of records; we achieved a 96 percent response rate. These surveys are extremely comprehensive and were developed over many months with assistance from agency privacy officials. Moreover, to help verify the accuracy of agencies' answers related to compliance, we randomly selected a sample of agency responses to the surveys and asked officials to provide documentation or additional narrative explanations to support their answers. We then invited key senior Privacy Act officials from all 25 agencies to discuss their responses at an all-day forum, where they had a chance to provide additional context for us before the preparation of the draft report. Overall, we consider this report to be a comprehensive and accurate source of information on agencies' implementation of the Privacy Act.

2. We disagree that our draft report, by treating the various provisions of the act as equally important, understates the extent of agency privacy protections. In passing the Privacy Act, Congress enacted a framework designed to protect personal privacy. Accordingly, we based our conclusions on the results of a comprehensive analysis of agency compliance with a broad range of requirements.

   As OMB suggests, we added to the body of our report a statement that agencies reported 100 percent compliance with our question concerning unauthorized access or disclosure of personal information contained in information systems. However, this response should not be interpreted as meaning that agencies fully complied with the Privacy Act's prohibitions against unauthorized disclosures. The question OMB cites is focused on information security controls for protecting personal information contained in information systems—which would not include the estimated 31 percent of systems of records that were exclusively paper records. Further, in response to another question, agencies acknowledged that in an estimated 21 percent of their systems

of records, they did not have the means to detect unauthorized intrusions into their information systems, drawing into question whether agencies have adequate means to determine whether or not there have been unauthorized disclosures. As discussed in our report, we have reported extensive weaknesses in information security across government.

3. We disagree that there is inconsistency between the survey responses on accounting for disclosures. The two questions asked were similar, but not identical. Therefore, there should be no expectation that the results would be identical. In our agency survey, we asked agencies a general question on whether they account for disclosures outside the agency for all systems of records. In the system of records survey, we asked agencies about their ability to account for *all* disclosures for a *specific* system of records that we randomly selected from the population.

4. Regarding our questions on maintaining complete, accurate, and relevant information, there are again major differences in these two questions that explain the differing results. One question asks how agencies maintain complete, accurate, and relevant information for *internal* agency determinations about an individual, while the other asks how this is done when providing information to a *nonfederal* organization. We do, however, agree with OMB that the readers of our report should see the multiple-choice answers that agencies could choose from in answering these questions and on which our compliance results are based. We have added them to the report.

5. Regarding OMB's concerns about questions that ask about particular activities undertaken in specific time frames, we note that these questions were directly derived from OMB's guidance to agencies. For example, we derived the question concerning reviews of *Federal Register* notices regarding systems of records directly from OMB's guidance. We support OMB in believing that such reviews help ensure that the public is informed of the existence and uses of systems of records and is thus able to access and amend records if necessary.

6. We agree with OMB regarding the question concerning review of training practices in fiscal year 2001. We removed this question from the report.

7. We disagree with OMB that there is a fundamental flaw in the draft report resulting from what is described as "the extremely limited nature and scope of the facts that GAO has actually reviewed." Our survey results represent 25 departments' and agencies' compliance with a broad range of Privacy Act provisions. Our surveys are extremely comprehensive, were developed over many months with assistance from agency privacy officials, and represent the population of 2,400 systems of records covering a broad cross section of small, medium, and large departments and agencies. Moreover, to help verify the accuracy of agencies' answers related to compliance, we randomly selected a sample of agency responses to the surveys and asked officials to provide documentation or additional narrative explanations to support their answers. We then invited key senior Privacy Act officials from all 25 agencies to discuss their responses at an all-day forum where they had a chance to provide additional context for us before the preparation of the draft report. Again, we consider this report to be a comprehensive and accurate source of information on agencies' implementation of the Privacy Act.

8. One of the first steps that we took when beginning this review of the Privacy Act was to contact agency Inspectors General for reports on the act. We found only a few reports, which were of limited scope. In addition, we acknowledge that GAO has not performed a comprehensive review of the Privacy Act in many years. However, as discussed in the draft report, we have issued reports over the past 3 years that raised concerns with the adequacy of selected OMB guidance concerning privacy. These reports contain outstanding recommendations to strengthen guidance, which OMB has not yet implemented.

9. One of the first steps we took when beginning this review was to examine the *Privacy Act Overview* from the Department of Justice and to meet with the Justice officials who prepared the overview. We used the overview, court decisions, and our interview with Justice officials to help frame some of the survey questions. However, a detailed analysis of these cases was not within the scope of our review nor necessary to address the objectives of our study. OMB appropriately pointed out that the individuals involved have the right to seek judicial review of agencies' compliance with the act; we discuss this point in the background section of our report.

10. In doing this work, our intention was to depict a governmentwide picture of agency compliance with the Privacy Act and OMB guidance. Although we present these results in the aggregate, they are based on reviews of 24 individual agencies and a representative sample of 2,400 systems of records. We will be providing OMB officials with additional details so that they can follow up with the specific agencies involved and ensure that deficiencies are corrected.

11. OMB's 1999 review did not require agencies to review all systems of records. Instead, OMB directed agencies to focus 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." The difference in the scope of OMB's review (selective) and ours (random sample) explains why agencies reported different results.

12. OMB commented that our draft report does not make clear what actions they should take because it does not point to any specific "deficiencies in compliance" at specific agencies or programs. The draft report contains specific compliance findings related to a broad range of Privacy Act requirements. As previously discussed, this information is presented in aggregate form; we will be providing additional details to help OMB in its improvement efforts.

    Regarding OMB guidance, the draft report identifies many of the specific deficiencies that agencies noted. We did not include the detailed deficiencies that agencies identified in response to OMB's January 1999 memorandum because OMB already had this information. Other specific deficiencies from our survey were previously shared with OMB officials. Nevertheless, we will be providing OMB officials with all the additional details on the specific deficiencies in OMB guidance that agencies identified in both the OMB and the GAO studies.

13. We disagree with OMB's comment that we never initiated a formal review with OMB, never requested the opportunity to interview OMB staff, and declined an invitation to review OMB activities. Consistent with GAO policy, we held an entrance conference with OMB on May 30, 2001, to initiate this review. At that meeting, we interviewed the key OMB officials who have Privacy Act responsibilities and asked them questions covering every aspect of this engagement. During the course of our review, we offered to share drafts of our surveys with OMB officials to obtain their views and suggestions; they declined this

opportunity. Since then we have been in frequent communication with OMB privacy officials to keep them apprised of our progress and, as OMB's comment acknowledges, shared with them the draft briefing slides that contained the interim results from our surveys. We met with them to discuss the briefing slides on November 14, 2002, and January 7, 2003.

Consistent with GAO policy, we also held an exit conference on April 3, 2003, to share our preliminary results and conclusions with OMB. At that meeting, OMB officials provided us with oral comments and stated that they would provide us with additional comments in writing; these written comments were not provided. As we began summarizing the results from our surveys and forum, we had several conversations with OMB officials, including a meeting on May 28, 2003, to discuss their concerns about our methodology and preliminary findings; many of the concerns were addressed as we drafted the final report.

Overall, OMB had many opportunities to provide us with additional evidence to support its view that our results and conclusions were inaccurate; however, it provided little additional information except to take issue with our study approach. In addition, we note that although we informed OMB of our survey approach early in our study, it chose to take issue with the approach only after we had obtained results.

GAO Contact and Staff Acknowledgments

GAO Contact

Alan Stapleton, (202) 512-3418

Staff Acknowledgments

In addition to the person named above, Bill Bates, Barbara Collier, Robert Crocker, John Dale, Neil Doherty, Wilfred Holloway, William Isrin, Michael Jarvis, Tuong-Vi La, Alison Martin, Luann Moy, David Noone, David Plocher, Mark Ramage, Terry Richardson, Theresa Roberson, and Warren Smith made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00