United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2008

# INFORMATION SECURITY

# Protecting Personally Identifiable Information


GAO-08-343

January 2008

# INFORMATION SECURITY

## Protecting Personally Identifiable Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-343, a report to congressional requesters

### Why GAO Did This Study

The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. As shown in prior GAO reports, compromises to such information and long-standing weaknesses in federal information security raise important questions about what steps federal agencies should take to prevent them. As the federal government obtains and processes information about individuals in increasingly diverse ways, properly protecting this information and respecting the privacy rights of individuals will remain critically important.

GAO was requested to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent guidance from the Office of Management and Budget (OMB) to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. To do so, GAO reviewed relevant laws and guidance, surveyed officials at 24 major federal agencies, and examined and analyzed agency documents, including policies, procedures, and plans. In commenting on a draft of this report, OMB stated that it generally agreed with the report's contents.

To view the full product, including the scope and methodology, click on GAO-08-343. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

### What GAO Found

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas, including minimum information security requirements for information and information systems. In the wake of recent incidents of security breaches involving personal data, OMB issued guidance in 2006 and 2007 reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter.

Not all agencies had developed the range of policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. Of 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the 24 agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information from improper disclosure.

At the conclusion of GAO's review, OMB announced in November 2007 that agencies that did not complete certain privacy and security requirements, including those just described, received a downgrade in their scores for progress in electronic government initiatives. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and GAO's previous recommendations on improving agency information security and implementation of FISMA requirements, GAO is making no further recommendations at this time.

# Contents

## Abbreviations

| | |
|---|---|
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act of 2002 |
| HIPPA | Health Insurance Portability and Accountability Act of 1996 |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIA | privacy impact assessment |
| US-CERT | U.S. Computer Emergency Readiness Team |
| VA | Department of Veterans Affairs |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

January 25, 2008

The Honorable Norm Coleman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan A. Davis
House of Representatives

Concerns regarding the security of personal information on federal systems have been raised by incidents in which such information has been compromised by the loss or theft of equipment or by unauthorized access. For example, in a reported incident involving the Department of Veterans Affairs, a laptop computer containing the personal data of millions of veterans was stolen from the home of an employee in May 2006. Similar incidents have occurred at other agencies, such as an incident at the Department of Energy, detected in mid 2005, when hackers gained access to more than 1,500 records, and another in June 2006, when the Department of Agriculture reported a hacker had broken into several systems that potentially compromised personal records for up to 26,000 people.

These security breaches highlight the importance of federal agencies having effective information security controls in place to protect personally identifiable information—that is, information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual. Loss of such information may lead to identity theft[1] or other fraudulent use of the information, resulting in substantial harm, embarrassment, and inconvenience to individuals.

As the federal government obtains and processes information about individuals in increasingly diverse ways, it is critically important that it ensure that the privacy rights of individuals are respected and this

[1]Identity theft is the wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.

information is properly secured and protected. Security breaches that compromise such information raise important questions about the steps that federal agencies should take to prevent them.

To help answer these questions, you asked us to (1) identify the federal laws enacted and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent Office of Management and Budget (OMB) guidance to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.

To address the first objective, we reviewed relevant laws and guidance and determined the requirements and recommended actions relevant to securing personally identifiable information. To address the second objective, we surveyed the 24 major federal agencies and departments,[2] and we examined and analyzed agency policies, procedures, plans, and artifacts against recent OMB guidance. Appendix I contains additional details on the objectives, scope, and methodology of our review. We conducted this performance audit from September 2006 to January 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Results in Brief

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Overall agency information security responsibilities are set forth in the Federal Information Security Management Act of 2002 (FISMA).[3] This act requires agencies to develop,

[2]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

[3]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act requires agencies, among other things, to develop risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level. In addition, to help agencies implement FISMA requirements, the act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas.[4] Accordingly, NIST has developed (1) standards for categorizing information and information systems so that agencies can provide appropriate levels of security according to risk levels (low, moderate, or high),[5] (2) guidelines recommending the types of information and information systems to be included in categories of risk,[6] and (3) minimum information security requirements for information and information systems in each category.[7] In the wake of recent incidents of security breaches involving personal data, OMB has issued guidance reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices, follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter, and establish core management groups to respond to security breaches involving personally identifiable information. OMB also updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information and directed agencies to develop policies for notifying those affected by such breaches.

Not all agencies had developed and documented policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported

[4]FISMA requires NIST to develop this guidance for systems other than national security systems.

[5]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard (FIPS) 199 (Washington, D.C., February 2004).

[6]NIST, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, Special Publication 800-60 (Washington, D.C., June 2004).

[7]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington, D.C., March 2006).

outside an agency's secured physical perimeter. Of the 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts for databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information from improper disclosure.

At the conclusion of our review, OMB announced that agencies that did not complete all the privacy and security requirements identified in a key OMB directive received a downgrade in their scores for E-Government progress on the President's Management Agenda Scorecard. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and our previous recommendations on improving agency information security and implementation of FISMA requirements,[8] we are making no further recommendations at this time.

In providing oral comments on a draft of this report, OMB representatives generally agreed with the report's contents.

## Background

The growth in information technology, networking, and electronic storage has made it ever easier to collect and maintain information about individuals. An accompanying growth in incidents of loss and unauthorized use of such information has led to increased concerns about protecting this information on federal systems. As a result, the basic law governing privacy protections, the Privacy Act of 1974, has been supplemented by more recent laws and guidance that are particularly

[8]GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

concerned with the protection of personally identifiable information maintained in automated information systems.[9]

Protecting personally identifiable information in federal systems is critical because its loss or unauthorized disclosure can lead to serious consequences for individuals. These consequences include identity theft or other fraudulent activity, which can result in substantial harm, embarrassment, and inconvenience. In 2006, the estimated losses associated with identity theft to U.S. organizations were $49.3 billion.[10]

## Incidents Have Placed Personal Information at Risk

Like other sectors, the federal government has seen significant exposures of personally identifiable information. According to a 2006 congressional staff report, since January 2003, 19 departments and agencies reported at least one loss of personally identifiable information that could expose individuals to identity theft.[11] (App. II provides selected examples of these and other incidents.)

A series of data breaches at federal agencies have involved system intrusion, phishing scams,[12] and the physical loss or theft of portable computers, hard drives, and disks. During fiscal year 2006, federal agencies reported a record number of incidents to the U.S. Computer Emergency Readiness Team (US-CERT). For example, in 2006 there were 5,146 incident reports—a substantial increase over the 3,569 incidents reported in 2005. During this period, US-CERT recorded a dramatic rise in incidents where either physical loss or theft or system compromise resulted in the loss of personally identifiable information.

[9]As used in this report, the term personally identifiable information is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

[10]GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07- 705 (Washington, D.C.: June 22, 2007).

[11]Committee on Government Reform, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C., Oct. 13, 2006).

[12]Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

## Weaknesses in Implementing Security Policies Have Persisted at Federal Agencies

As illustrated by recent security incidents and as we have previously reported,[13] significant weaknesses continued to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies indicated that deficient information security controls were either a reportable condition[14] or a material weakness.[15] Our audits continue to identify similar weaknesses in nonfinancial systems. Similarly, in their annual reporting under 31 U.S.C. § 3512 (commonly referred to as the Federal Managers' Financial Integrity Act of 1982),[16] 17 of 24 agencies reported shortcomings in information security, including 7 that considered it a material weakness. Agency inspectors general have also noted the seriousness of information security, with 21 of 24 including it as a "major management challenge" for their agencies.[17]

According to our reports and those of inspectors general, persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs

[13]See GAO-07-837.

[14]Reportable conditions are significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[15]A material weakness is a reportable condition that precludes the entity's internal controls from providing reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

[16]FMFIA (31 U.S.C. § 3512) requires agencies to report annually to the President and Congress on the effectiveness of internal controls and any identified material weaknesses in those controls. Per OMB, for the purposes of FMFIA reporting, a material weakness also encompasses weaknesses found in program operations and compliance with applicable laws and regulations. Material weaknesses for FMFIA reporting are determined by management, whereas material weaknesses reported as part of a financial statement audit are determined by independent auditors.

[17]The Reports Consolidation Act of 2000 (31 U.S.C. § 3516(d)) requires inspectors general to include in their agencies' performance and accountability report a statement that summarizes what they consider to be the most serious management and performance challenges facing their agency and briefly assesses their agencies' progress in addressing those challenges.

are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Most agencies had weaknesses in each of these categories. Accordingly, we have designated information security as a governmentwide high-risk issue in reports to Congress since 1997—a designation that remains in force today.[18]

## Federal Laws and Guidance Provide a Foundation for Agencies to Protect Personally Identifiable Information

The primary laws that provide privacy protections to personal information are the Privacy Act of 1974 and the E-Government Act of 2002; these laws describe, among other things, agency responsibilities with regard to personally identifiable information, which include providing security. The security of information held by the federal government is specifically addressed by FISMA, which requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems, including personally identifiable information. Along with technical guidance from NIST, FISMA establishes a risk-based approach to security management, which requires an agency, among other things, to categorize its information and systems according to the potential impact to the agency should the information be jeopardized. In the wake of recent incidents of security breaches involving personal data, OMB has issued guidance reiterating the requirements of these laws and guidance, drawing particular attention to those associated with personally identifiable information. In addition, OMB updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information.

[18]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

## Privacy and Security of Personal Information Are Addressed in Several Federal Laws

The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.[19] In addition, FISMA, which is included in the E-Government Act of 2002, addresses the protection of personal information in the context of securing federal agency information and information systems.

To protect personal privacy, the Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a notice in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.[20] The act's requirements also apply to government contractors when agencies contract for the development and maintenance of a system of records to accomplish an agency function.[21]

The provisions of the Privacy Act are consistent with and based primarily on a set of principles for protecting the privacy and security of personal

[19]No single federal law governs all uses of personally identifiable information. In addition to the laws that govern federal agency use of such information, a number of statutes provide privacy protections for information used for specific purposes or maintained by specific types of entities. For example, the Fair Credit Reporting Act applies to companies that prepare or furnish information on consumer creditworthiness, and the Video Privacy Protection Act applies to the use of video rental records.

[20]Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[21]5 U.S.C. § 552a(m)(1).

information—the Fair Information Practices.[22] These principles have been widely adopted as the standard benchmark for evaluating the adequacy of privacy protections; one of the principles is security safeguards.[23] In this regard, the Privacy Act requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[24]

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[25] a PIA is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form or (2) before initiating any new data collections involving personal information that will be

[22]These principles were first proposed in 1973 by a U.S. government advisory committee; they were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. The practices include principles such as security safeguards (personally identifiable information should be protected with reasonable security safeguards), openness (the public should be kept informed about privacy policies and practices), and accountability (those controlling the collection or use of personally identifiable information should be accountable for taking steps to ensure the implementation of these principles). Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C., July 1973).

[23]Others include data quality, openness, individual participation, and use limitation.

[24]5 U.S.C. § 552a(e)(10).

[25]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is being used. The PIA requirement does not apply to all systems. For example, no assessment is required when the information collected relates to internal government operations, the information has been previously assessed under an evaluation similar to a PIA, or when privacy issues are unchanged.

Besides these primary laws, Congress has passed laws requiring protection of personally identifiable information that are agency-specific or that target a specific type of information. For example, the Veterans Benefits, Health Care, and Information Technology Act,[26] enacted in December 2006, establishes information technology security requirements for personally identifiable information that apply specifically to the Department of Veterans Affairs (VA). The act mandates, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving personally identifiable information; and, if necessary, provide credit protection services to those individuals whose personally identifiable information has been compromised. Another example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[27] which requires the Secretary of Health and Human Services to adopt standards for the electronic exchange, privacy, and security of health information. These standards apply to agencies, such as the Department of Defense and VA, to the extent they are covered by HIPAA.

FISMA is the primary law governing information security in the federal government; it also addresses the protection of personal information in the context of securing federal agency information and information systems. FISMA, which establishes a risk-based approach to security management, defines federal requirements for securing information and information systems that support federal agency operations and assets. Under the act, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and

[26] Pub. L. No. 109-461 (Dec. 22, 2006).

[27] Pub. L. No. 104-191 (Aug. 21, 1996).

disclosure (and thus to protect personal privacy, among other things). The act also requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency (including those provided or managed by another agency, contractor, or other source).

Specifically, the act requires that these information security programs include, among other things,

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, FISMA requires agencies to produce an annually updated inventory of major information systems (including major national security systems) operated by the agency or that are under its control, which includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

Like protecting other information and systems, protecting personally identifiable information is dependent on agencies' having established security programs that include the elements described above. Among other things, agencies must identify the personally identifiable information in their information systems, determine the appropriate risk level associated with it, develop appropriate controls to secure it, and ensure that these controls are applied and maintained.

FISMA also establishes evaluation and reporting requirements. Under the act, each agency must have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency inspectors general or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

FISMA also requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices, and compliance with the act's requirements. In addition, agency heads are required to annually report the results of their independent evaluations to OMB.[28] OMB is required to submit a report to Congress each year on agency compliance with the act's requirements, including a summary of findings of agencies' independent evaluations.

## FISMA Requires NIST to Develop Security Guidance

Other major FISMA provisions require NIST to develop, for systems other than national security systems, standards for categorizing information and information systems according to risk levels, guidelines on the types of information and information systems that should be included in each category, and standards for minimum information security requirements

[28]Except that, to the extent an evaluation pertains to a national security system, only a summary and assessment of that portion of the evaluation is reported to OMB.

for information and information systems in each category. Accordingly, NIST developed the following guidance:

- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. This standard is to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. In addition, NIST has published Special Publication 800-60, to provide guidance on how to implement FIPS 199 and how to determine whether a system or information should be categorized as having a high-, moderate-, or low-risk impact level.

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. This standard provides minimum information security requirements for information and information systems in each risk category.

- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The publication provides guidelines for selecting and specifying security controls for information systems supporting the federal government.

## OMB Provides Guidance Reiterating Requirements on Security and Privacy

OMB is responsible for establishing governmentwide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws. It has issued both recommended steps and required actions to protect federally owned information and information systems. For example, OMB memorandum M-05-08[29] directs agencies to designate a senior official with overall responsibility for information privacy issues, including taking appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing, and to protect related information systems from unauthorized access, modification, disruption, or destruction.

Following the May 2006 VA data breach, OMB issued guidance reiterating agency responsibilities under the laws and technical guidance, drawing

[29]OMB, *Designation of Senior Agency Officials for Privacy*, memorandum M-05-08 (Washington, D.C., Feb. 11, 2005).

particular attention to the requirements associated with personally identifiable information.

OMB memorandum M-06-15, *Safeguarding Personally Identifiable Information*, re-emphasizes agency responsibilities to safeguard personally identifiable information and to appropriately train employees in this regard. It also requires agencies to perform a review of their policies and procedures for the protection of personally identifiable information, including an examination of physical security, and to take corrective action.

OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, asks agencies to verify that existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed. It recommends, among other things, that all information on mobile computers and devices be encrypted unless a written waiver is issued certifying that the computer does not contain any sensitive information. In addition, M-06-16 recommends that agencies use a NIST checklist included in the memorandum. The NIST checklist states that agencies should verify that information requiring protection as personally identifiable information is appropriately categorized as such and that it is assigned an appropriate risk impact category.

OMB also updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information. OMB memorandum M-06-19 directs agencies to report all incidents involving personally identifiable information to US-CERT within 1 hour of discovery of the incident. Further, OMB recommends that agencies establish a core management group responsible for responding to the loss of personal information in a memorandum issued September 20, 2006. In OMB memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB asks agencies to identify in their yearly FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information. In these annual reports, agencies also are required to report numbers of incidents for the reporting period, the number of incidents the agency reported to US-CERT, and the number reported to law enforcement.

Most recently, OMB memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to develop and implement breach notification policies—

that is, policies governing how and under what circumstances affected parties are notified in case of a security breach. Agencies were to develop and implement such policies and associated plans within 120 days from the issuance of the memorandum (May 22, 2007).

The memorandum also reiterates four particularly important existing security requirements that agencies should already have been implementing: (1) assigning an impact level to all information and information systems, (2) implementing the minimum security requirements and controls in FIPS 200 and NIST Special Publication 800-53 respectively, (3) certifying and accrediting information systems, and (4) training employees. With regard to the first of these, OMB stressed that agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

In addition, this memorandum reiterates the guidance provided in memorandum M-06-16 on protection of personally identifiable information and changes earlier recommendations to requirements.

These and other OMB memorandums significant to the protection of personally identifiable information are briefly described in table 1.

**Table 1: Major OMB Memorandums Related to Protection of Personally Identifiable Information**

| Memorandum, date | Title | Major personally identifiable information requirement or recommendation |
|---|---|---|
| M-05-08, Feb. 11, 2005 | Designation of Senior Agency Officials for Privacy | Directs agencies to designate a senior official with overall responsibility for information privacy issues who<br>• is accountable for ensuring agency implementation of information privacy protection; and<br>• must take appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing, and to protect related information systems from unauthorized access, modification, disruption, or destruction. |
| M-06-15, May 22, 2006 | Safeguarding Personally Identifiable information | Re-emphasizes agency responsibilities to safeguard personally identifiable information and to appropriately train employees in this regard.<br>Requires agency Senior Official for Privacy to conduct a review of policies and processes, and take necessary corrective actions to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. |

| Memorandum, date | Title | Major personally identifiable information requirement or recommendation |
|---|---|---|
| M-06-16, June 23, 2006 | Protection of Sensitive Agency Information | Recommends that all agencies<br>• encrypt all data on mobile computers/devices that carry agency data unless the data are determined to be nonsensitive;<br>• allow remote access only with two-factor authentication, where one factor is provided by a device separate from the computer gaining access;<br>• use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity; and<br>• log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days.<br>Recommends that agencies use a NIST security checklist, included in the memo, that provides specific actions to be taken by agencies to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. |
| M-06-19, July 12, 2006 | Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments | Requires agencies to report all incidents involving personally identifiable information to US-CERT within 1 hour of discovering the incident (this revises previous guidelines for reporting security incidents). |
| M-06-20, July 17, 2006 | FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management | Requires agencies to identify in their yearly FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information. |
| M-07-16, May 22, 2007 | Safeguarding Against and Responding to the Breach of Personally Identifiable Information | Requires agencies to develop and implement a breach notification policy and plan, including policy for the notification of the public, and provides the elements that must be included in the policies, including the incident reporting requirements of M-06-19.<br>Restates recommendations of M-06-16 as requirements.<br>Requires agencies to establish an agency response team to ensure adequate coverage and implementation of the plan.<br>Requires agencies to review and reduce the volume of personally identifiable information to the minimum necessary and reduce the use of Social Security numbers.<br>Updates incident reporting and handling requirements.<br>Requires agencies' breach notification policy and plan to lay out employees' roles and responsibilities for handling breaches of personally identifiable information, as well as relationships with contractors or partners. |

Source: GAO analysis of OMB memorandums.

## Not All Agencies Had Developed Policies and Procedures Reflecting OMB Guidance on Protection of Personally Identifiable Information

Ensuring that agency policies and procedures appropriately emphasize the protection of personally identifiable information in accordance with applicable laws and guidance is an important aspect of protecting personal privacy. In recent guidance, OMB directed agencies to encrypt and otherwise protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.[30] Specifically, agencies were required to

- encrypt[31] all data on mobile computers or devices that carry agency data, unless the data are determined to be nonsensitive;
- allow remote access only with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access;
- use a "time-out" function for remote access and mobile devices that requires that users re-authenticate after 30 minutes of inactivity; and
- log all instances in which computer-readable data are extracted from databases holding sensitive information, and verify that each extract including sensitive data has been erased within 90 days or that its use is still required.

OMB also recommended the use of a NIST-provided checklist for the protection of remote information, which was included in memorandum M-06-16. The checklist provides specific actions to be taken by federal agencies for the protection of personally identifiable information that is categorized as moderate or high impact and that is either accessed remotely or physically transported outside an agency's secured, physical perimeter, including information transported on removable media and on portable or mobile devices such as laptop computers and personal digital assistants. The controls and assessment methods and procedures in the checklist are a subset of what is currently required under NIST Special Publications 800-53 and 800-53A for moderate- and high-impact information systems. In addition, NIST standard (FIPS 140-2, *Security Requirements for Cryptographic Modules*) is to be used by federal

[30]OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, presented this guidance as recommendations. OMB memorandum M-07-16 established the recommendations as requirements.

[31]Encryption is a method of providing basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm.

organizations when it is specified that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. All encryption modules that protect sensitive data must follow this standard.

However, not all agencies had developed policies and procedures reflecting OMB guidance for protecting personally identifiable information that is accessed remotely or physically transported outside an agency's secured perimeter. Of the 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. A smaller number of agencies had policies to provide other protections recommended by OMB, 14 of the agencies had two-factor authentication policies for remote access. Fifteen of the agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. One agency used a reauthentication time shorter than 30 minutes (15 minutes). Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. However, several of the agencies that had not established such policies indicated that they were researching technical solutions to address these issues.

Four agencies had policies requiring the use of the NIST checklist recommended by OMB. In addition, 20 agencies had written policies that require encryption software to be NIST FIPS 140-2 compliant.[32]

Gaps in their policies and procedures reduce agencies' ability to protect personally identifiable information from improper disclosure. The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because agencies maintain significant amounts of information concerning individuals, agencies should be more vigilant to protect that information from loss and misuse.

At the conclusion of our review and with the recent release of OMB's President's Management Agenda Scorecard for the fourth quarter of fiscal year 2007, OMB announced that agencies that did not complete all the

[32]NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Washington, D.C., May 2001).

privacy and security requirements identified in OMB memorandum M-07-16, which included the requirements just described, received a downgrade in their scores for E-Government progress. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area, we are making no recommendations at this time.

We reiterate, however, as we have in the past, that although having specific policies and procedures in place is an important factor in helping agencies to secure their information systems and to protect personally identifiable information, proper implementation of these policies and procedures remains crucial. Agencies' implementation of OMB's guidance on personally identifiable information, as well as our previous recommendations on improving agency information security and implementation of FISMA requirements,[33] will be essential in improving the protection of personally identifiable information.

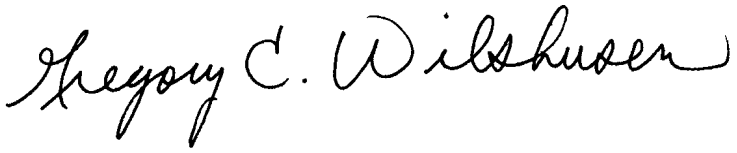
## Agency Comments

In providing oral comments on a draft of this report, OMB representatives stated that they generally agreed with the report's contents. In addition, they provided technical comments that we incorporated into the report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at www.gao.gov.

[33]See GAO-07-837. This report noted that almost all of the 24 major federal agencies had weaknesses in one or more areas of information security controls, including preventing, limiting, or detecting access to computer networks, systems, or information.

If you have questions about this report, please contact me at (202) 512-6244. I can also be reached by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' policies and documented procedures that respond to recent Office of Management and Budget (OMB) guidance to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.

To address our first objective, we identified and reviewed legislative requirements for the protection of personally identifiable information by federal agencies. Specifically, we reviewed

- the Privacy Act of 1974;
- the E-Government Act of 2002;
- the Federal Information Security Management Act of 2002;
- the Veterans Benefits, Health Care, and Information Technology Act of 2006; and
- the Health Insurance Portability and Accountability Act of 1996.

We also reviewed policy and guidance issued by OMB[1] and National Institute of Standards and Technology (NIST) relevant to agencies' policies and procedures to safeguard personally identifiable information.

To address our second objective, we selected 24 major agencies and assessed the status of their policies and procedures addressing recent OMB guidance addressing personally identifiable information.[2] At our request, each agency completed a survey of personally identifiable information practices and provided related policies and procedures. The survey and document request were based on requirements and

[1]See table 1 for a description of relevant OMB memorandums.

[2]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

recommendations in the OMB guidance. We examined survey responses and compared agency-documented policies and procedures to OMB's requirements and guidance for consistency and sufficiency. We did not evaluate the effectiveness of agencies' implementation of the practices. However, we reviewed applicable prior GAO and agency inspector general reports and discussed whether agency policies had been fully implemented with applicable agency information technology officials.

We conducted this performance audit from September 2006 to January 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Selected Government Data Breach Incidents, November 2004 through January 2007

The incidents noted here were reported by government agencies between November 2004 and January 2007. Many of these incidents included the loss of personally identifiable information. These incidents were selected to provide illustrative examples of the types of incidents that occurred during this period.

- November 3, 2004, Department of Education: information of 8,290 individuals lost in the mail

  A contractor to the Federal Student Aid program sent the personal information of 8,290 individuals via a commercial shipping company. After determining that the package had been lost in transit, the department decided not to notify the affected individuals. It discontinued using that carrier for that facility as a result.

- November 24, 2004, Department of Veterans Affairs (VA): personal information accidentally disclosed on public drive of VA e-mail system

  A public drive on a VA e-mail system permitted entry by all users to folders and files containing personally identifiable information (name, Social Security number, date of birth, and in some cases personal health information such as surgery schedules, diagnosis, status, etc.) of veterans after computer system changes were made. All folders were then restricted and the individual services were contacted to limit user access.

- December 6, 2004, Department of Veterans Affairs: two personal computers stolen, exposing data of 2,000 research subjects

  Two desktop personal computers were stolen from a locked office in the research office of a medical center. One of the computers had files containing names, Social Security numbers, next of kin, addresses, and phone numbers of approximately 2,000 research subjects. The computers were password protected by the standard VA password system. The medical center immediately contacted the agency privacy officer for guidance. Letters were mailed to all research subjects informing them of the computer theft and potential for identity theft. VA enclosed letters addressed to three major credit agencies and postage paid envelopes. This incident was reported to VA and federal incident offices.

- December 17, 2004, Department of Agriculture: e-mail sent out to 1,537 individuals whose personally identifiable information was potentially exposed

An e-mail was sent to 1,537 people that included an attachment with the Social Security numbers and other personal information of all 1,537 individuals. In response to the event, a letter of apology was sent and training on appropriate security measures was developed.

- February 24, 2005, Department of Agriculture: hacker obtains access

  A system containing research data was breached when someone cracking a password or a user account installed hacking software. The agency reports that no data were compromised but that the hacker had read and write access to the server and opened access points.

- March 4, 2005, Department of Veterans Affairs: list of Social Security numbers of 897 providers inadvertently sent via e-mail

  An employee reported e-mailing a list of the names and Social Security numbers of 897 providers to a new transcription company. This was immediately reported and a supervisor called the transcription company and spoke with the owner and requested that the company destroy the file immediately. Notification letters were sent out to all 897 providers. Disciplinary action was taken against the employee.

- June 17, 2005, Department of Defense: potential unauthorized access found

  A systems administrator discovered potential unauthorized access to the Air Force Personnel Center Assignment Management System with personally identifiable information on 33,000 military members. Notifications were sent out to system users and an investigation was begun.

- Mid 2005, Department of Energy: a hacker accessed more than 1,500 records

  In June 2006, it was announced a hacker had gained access to a file containing the names and Social Security numbers of 1,502 individuals. This event, which was detected in mid 2005, was not reported to senior Department officials until June 2006.

- October 14, 2005, Department of Veterans Affairs: personal computer stolen, exposing data on 421 patients

A personal computer was stolen from a medical center that contained information on 421 patients and included patient names, last four digits of their Social Security number, height, weight, allergies, medications, recent lab results, and diagnoses. The agency's privacy officer and medical center information security officer were notified. The use of credit monitoring was investigated and it was determined that, because the entire Social Security number was not listed, it would not be necessary to use these services at the time.

- November 5, 2005, Department of Education: personally identifiable information of 11,329 student borrowers lost

  The unencrypted magnetic tape was lost from the Federal Student Aid's Virtual Data Center. After an investigation, no criminal activity was found and the case was closed.

- November 18, 2005, Department of Health and Human Services: contractor employees steal records of approximately 1,574

  Two employees of the Centers for Medicare & Medicaid Services contractor stole records for the purpose of identity theft. The approximately 1,574 individuals were notified.

- February 15, 2006, Department of Health and Human Services: 22 laptops stolen from contractor site, exposing information on 1,382

  The Centers for Disease Control and Prevention reported 22 laptops stolen from a contractor's facility; 3 of them contained Department of Defense service member information affecting 1,382 personnel. All of the potentially impacted individuals were notified.

- March 17, 2006, Department of Defense: thumb drive with personally identifiable information of approximately 207,570 Marines lost

  The information on approximately 207,570 enlisted Marines from 2001 to 2005 was lost. A notification letter was sent to the affected individuals and the Marine Corps.

- March 28, 2006, Department of Health and Human Services: eight laptops stolen from contractor, exposing information on 10,855

Eight laptops containing beneficiary and supplier information were stolen from the contractor's office. The beneficiary list on the laptops included 10,855 names, addresses, and dates of birth.

- April 5, 2006, Department of Defense: hackers access Tricare Management Activity, exposing personal data

  Hackers accessed a system containing personally identifiable information on military employees. Approximately 14,000 active duty and retired service members and dependents were affected and notified. New security measures were implemented.

- April 11, 2006, Department of Veterans Affairs: hacker and employee compromise systems, exposing information on 79,000 veterans

  A former VA employee was suspected of hacking into a medical center computer system with the assistance of a current employee who provided rotating administrator passwords. All systems in the medical center serving 79,000 veterans were compromised.

- May 3, 2006, Department of Veterans Affairs: computer equipment containing personally identifiable information of approximately 26.5 million veterans and active duty members of the military was stolen

  Computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee.

- June 3, 2006, Department of Agriculture: systems compromised and potentially exposed information on 26,000

  Three Department of Agriculture computers system were compromised, potentially exposing the personally identifiable information of 26,000 individuals, including photographs. The department notified the individuals.

- June 19, 2006, Department of Education: package with personally identifiable information of 13,700 study respondents lost

  The shipping contractor to the department's National Center for Education Statistics lost a package containing the personally identifiable information of 13,700 study respondents.

- June 22, 2006, Department of Health and Human Services: laptop stolen from contractor employee, exposing information on 49,572

  The theft of a contractor employee's laptop containing a variety of personally identifiable information including medical information was reported. A total of 49,572 Medicare beneficiaries may have been affected. All were notified.

- July 1, 2006, Department of Commerce: documents and database copied by a former employee, exposing 934 employees

  A former employee copied sensitive letters and a database of employee information. The database included information on 883 cases and the letters had medical information on 51 employees.

- July 27, 2006, Department of Transportation: laptop stolen from car of DOT Inspector General, exposing information on approximately 133,000

  A laptop containing personally identifiable information of approximately 133,000 Florida pilots, commercial drivers, and other Florida residents was stolen from a government-owned vehicle.

- August 1, 2006, Department of Defense: laptop falls off motorcycle, losing personally identifiable information of 30,000

  A laptop containing personally identifiable information on 30,000 applicants, recruiters, and prospects fell off a motorcycle belonging to a Navy recruiter.

- August 3, 2006, Department of Veterans Affairs: desktop computer stolen, exposing financial records of approximately 18,000 patients

  A desktop computer was stolen from a secured area at a contractor's facility in Virginia that processes financial accounts for VA. The desktop computer was not encrypted. Notification letters were mailed and credit monitoring services offered.

- September 6, 2006, Department of Veterans Affairs: laptop stolen, exposing patient information on an unknown number of individuals

  A laptop attached to a medical device was stolen. The information on an unknown number of individuals was exposed. Notification letters and credit protection services were offered to 1,575 patients.

- January 22, 2007, Department of Veterans Affairs: external hard drive missing or stolen, exposing records on 535,000 veterans and 1.3 million non-VA physician provider records

  An external hard drive was discovered missing or stolen, exposing records on 535,000 veterans and 1.3 million non-VA physician provider records from a research facility in Birmingham, Alabama. Notification letters were sent to veterans and providers, and credit monitoring services were offered to those individuals whose records contained personally identifiable information.

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

## Staff Acknowledgments

In addition to the individual named above, Shaun Byrnes, Barbara Collier, Susan Czachor, Kristi Dorsey, Nancy Glover, Joshua Hammerstein, Anthony Molet, David Plocher, Charles Vrabel (Assistant Director), and Jeffrey Woodward were key contributors to this report.

## GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

## 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. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 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

## Congressional Relations

Gloria Jarmon, Managing Director, jarmong@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548