United States Government Accountability Office

GAO

Report to Congressional Committees

July 2007

INFORMATION SECURITY

Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses

GAO-07-837

July 2007

INFORMATION SECURITY

Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-837, a report to congressional committees

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem with potentially devastating consequences—such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information—and has identified information security as a governmentwide high-risk issue.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies.

As required by FISMA to report periodically to Congress, in this report GAO discusses the adequacy and effectiveness of agencies' information security policies and practices and agencies' implementation of FISMA requirements. To address these objectives, GAO analyzed agency, inspectors general (IG), Office of Management and Budget (OMB), congressional, and GAO reports on information security.

What GAO Recommends

GAO is recommending that OMB strengthen FISMA reporting metrics. OMB agreed to take GAO's recommendations under advisement when modifying its FISMA reporting instructions.

www.gao.gov/cgi-bin/getrpt?GAO-07-837.

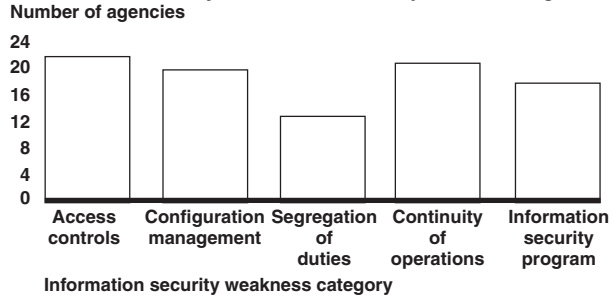
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Significant weaknesses in information security policies and practices threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. Recently reported incidents at federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to loss of privacy and identity theft. Almost all of the major federal agencies had weaknesses in one or more areas of information security controls (see figure). Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer resources. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; or maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully implemented their information security programs. As a result, agencies may not have assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006, agencies generally reported performing various control activities for an increasing percentage of their systems and personnel. However, IGs at several agencies disagreed with the information the agency reported and identified weaknesses in the processes used to implement these activities. Further, although OMB enhanced its reporting instructions to agencies for preparing fiscal year 2006 FISMA reports, the metrics specified in the instructions do not measure how effectively agencies are performing various activities, and there are no requirements to report on a key activity. As a result, reporting may not adequately reflect the status of agency implementation of required information security policies and procedures.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis of IG, agency, and GAO reports.

Contents

Figures

Abbreviations

BPD	Bureau of the Public Debt
CIO	chief information officer
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FISMA	Federal Information Security Management Act
FBI	Federal Bureau of Investigation
FRB	Federal Reserve Bank
HHS	Department of Health and Human Services
IG	inspector(s) general
IRS	Internal Revenue Service
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 27, 2007

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Henry A. Waxman
Chairman
The Honorable Tom Davis
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information. In reports to Congress since 1997, we have designated information security as a governmentwide high-risk issue—a designation that remains in force today.[1]

Concerned with accounts of attacks on systems through the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002.[2] To address information security weaknesses, FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. In addition, it provides a mechanism for improved oversight of federal agency information security programs. This mechanism includes mandated annual reporting by the agencies, the Office of Management and

[1]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).

[2]*Federal Information Security Management Act of 2002*, Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

Budget (OMB), and the National Institute of Standards and Technology (NIST). FISMA also includes a requirement for independent annual evaluations by the agencies' inspectors general (IG) or independent external auditors.

In accordance with the FISMA requirement that we report periodically to Congress, our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) their implementation of FISMA requirements. To address these objectives, we analyzed agency, IG, OMB, congressional, and our reports on information security. We conducted our evaluation from October 2006 through May 2007 in accordance with generally accepted government auditing standards. Our objectives, scope, and methodology, are further explained in appendix I.

Results in Brief

Significant weaknesses in information security policies and practices threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. Recently reported information security incidents at federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to loss of privacy and potential harm associated with identity theft. Almost all of the 24 major federal agencies[3] had weaknesses in one or more areas of information security controls. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply encryption to protect sensitive data on networks and portable devices; (5) log, audit, and monitor security-relevant events; and (6) restrict physical access to information assets. In

[3]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.

addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, agencies may not have assurance that controls are in place and operating as intended to protect their information and information systems, thereby leaving them vulnerable to attack or compromise.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006, agencies generally reported performing various required control activities for an increasing percentage of their systems and personnel. However, agency IGs at several agencies sometimes disagreed with the information the agency reported and identified weaknesses in the processes used to implement these activities. Pursuant to its FISMA responsibilities, NIST has issued federal standards and guidance on information security. Agency IGs have performed their annual independent evaluations of agencies' information security programs although the scope and methodologies of their evaluations varied across the agencies. Further, although OMB enhanced its reporting instructions to agencies for preparing their FISMA reports, the metrics specified in the instructions do not measure how effectively agencies are performing key activities, and there are no requirements to report on patch management—another key activity. As a result, reporting may not adequately reflect the status of agency implementation of required information security policies and procedures.

In prior reports, we have made hundreds of recommendations to agencies to address specific information security weaknesses. We are making recommendations to the Director of OMB to update its reporting instructions and to request that IGs evaluate certain FISMA implementation efforts. In commenting on a draft of this report, OMB agreed to take our recommendations under advisement when modifying its FISMA reporting instructions. OMB also noted that its current instructions provide the flexibility for IGs to tailor evaluations based on agency's documented weaknesses and plans for improvement.

Background

Federal agencies increasingly rely on computerized information systems and electronic data to conduct operations and carry out their missions. Protecting federal computer systems has never been more important due to advances in the sophistication and effectiveness of attack technology and methods, the rapid growth of zero-day exploits[4] and attacks, and the increasing number of security incidents occurring at organizations and federal agencies.

Information security is especially important for federal agencies, which increasingly use information systems to deliver services to the public and to ensure the confidentiality, integrity, and availability of information and information systems. Without proper safeguards, there is risk of data theft, compromise, or loss by individuals and groups due to negligence or malicious intent within or outside of the organization.

To fully understand the potential significance of information security weaknesses, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. The weaknesses place a broad array of federal operations and assets at risk. For example,

- Resources, such as federal payments and collections, could be lost or stolen.
- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of industrial espionage or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud, identity theft, or disruption.

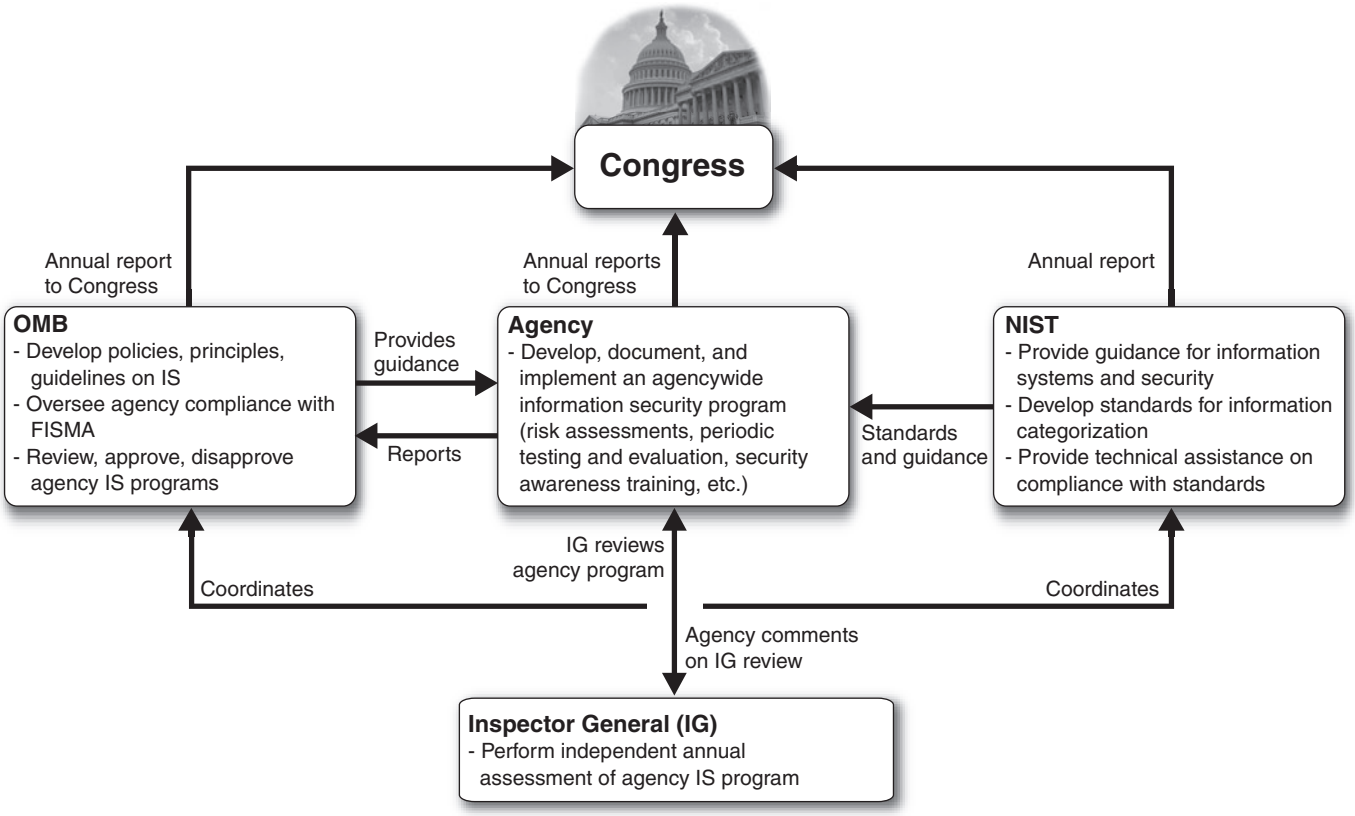
[4]A zero-day exploit takes advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public.

- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Recognizing the importance of securing federal systems and data, Congress passed FISMA in 2002, which set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program, and these activities are similar to the principles noted in our study of the risk management activities of leading private sector organizations[5]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. In order to ensure the implementation of this framework, the act assigns specific responsibilities to agency heads, chief information officers (CIO), IGs, and NIST (depicted in fig. 1). It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing agency information security programs, at least annually, and approving or disapproving them.

[5]GAO, *Executive Guide: Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

Figure 1: Division of FISMA Responsibilities



Source: GAO analysis of FISMA and implementing guidance.

Agency Responsibilities

FISMA requires each agency, including agencies with national security systems, 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, it requires information security programs that, among other things, include

- 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, agencies must produce an annually updated inventory of major information systems (including major national security systems) operated by the agency or 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.

FISMA also requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. In addition, agency heads are required to report

annually the results of their independent evaluations to OMB, except to the extent that an evaluation pertains to a national security system; then only a summary and assessment of that portion of the evaluation needs to be reported to OMB.

Responsibilities of the IG

Under FISMA, the IG for each agency must perform an independent annual evaluation of the agency's information security program and practices. The evaluation should include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. In addition, the evaluation must include an assessment of the compliance with the act and any related information security policies, procedures, standards, and guidelines. For agencies without an IG, evaluations of nonnational security systems must be performed by an independent external auditor. Evaluations related to national security systems are to be performed by an entity designated by the agency head.

Responsibilities of NIST

Under FISMA, NIST is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum (1) standards 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; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST must also develop a definition of and guidelines for detection and handling of information security incidents as well as guidelines, developed in conjunction with the Department of Defense and the National Security Agency, for identifying an information system as a national security system.

The law also assigns other information security functions to NIST, including

- providing technical assistance to agencies on such elements as compliance with the standards and guidelines and the detection and handling of information security incidents;

- evaluating private-sector information security policies and practices and commercially available information technologies to assess potential application by agencies;

- evaluating security policies and practices developed for national security systems to assess their potential application by agencies; and

- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.

NIST is also required to prepare an annual public report on activities undertaken in the previous year and planned for the coming year.

Responsibilities of OMB

FISMA states that the Director of OMB shall oversee agency information security policies and practices, including

- developing and overseeing the implementation of policies, principles, standards, and guidelines on information security;

- requiring agencies to identify and provide information security protections commensurate with risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, or information systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency;

- coordinating information security policies and procedures with related information resource management policies and procedures;

- overseeing agency compliance with FISMA to enforce accountability; and

- reviewing at least annually, and approving or disapproving, agency information security programs. In addition, the act requires that OMB report to Congress no later than March 1 of each year on agency compliance with FISMA.

Persistent Weaknesses Place Sensitive Data at Significant Risk

Significant control weaknesses in information security policies and practices threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. These persistent weaknesses expose sensitive data to significant risk, as illustrated by recent reported incidents at various agencies. Further, our work and reviews by IGs note significant information security control deficiencies that place a broad array of federal operations and assets at risk.

Incidents Place Sensitive Information at Risk

Since January 2006, federal agencies have reported a spate of security incidents that have put sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to loss of privacy and potential harm associated with identity theft. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following reported examples illustrate that a broad array of federal information and assets are at risk.

- The Department of Veterans Affairs (VA) announced that 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. Until the equipment was recovered, veterans did not know whether their information was likely to be misused. In June, VA sent notices to the affected individuals that explained the breach and offered advice on steps to take to reduce the risk of identity theft. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.

- A Centers for Medicare and Medicaid Services contractor reported the theft of a contractor employee's laptop computer from his office. The computer contained personal information including names, telephone numbers, medical record numbers, and dates of birth of 49,572 Medicare beneficiaries.

- The Department of Agriculture (USDA) was notified that it had posted personal information on a Web site. Analysis by USDA later determined that the posting had affected approximately 38,700 individuals, who had been awarded funds through the Farm Service Agency or USDA Rural Development program. That same day, all identification numbers associated with USDA funding were removed from the Web site. USDA is

continuing its effort to identify and contact all persons who may have been affected.

- A contractor for USDA's Farm Services Agency inadvertently released informational compact discs that contained Social Security numbers and tax identification data on approximately 350,000 tobacco producers/contract holders under the agency's Tobacco Transition Payment Program.

- The Transportation Security Administration (TSA) announced a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data, such as Social Security number, date of birth, payroll information, and bank account and routing information, was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.

- The Census Bureau reported 672 missing laptops, of which 246 contained some degree of personal data. Of the missing laptops containing personal information, almost half (104) were stolen, often from employees' vehicles, and another 113 were not returned by former employees. Commerce reported that employees were not held accountable for not returning their laptops, but the department did not report on the disposition of the remaining 29.

- Officials at the Department of Commerce's Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but they were unable to clearly define the amount of time that perpetrators were inside the department's computers, or find any evidence to show that data was lost as a result.

- The Department of Defense (Navy) Marine Corps reported the loss of a thumb drive containing personally identifiable information—names, Social Security numbers, and other information—of 207,570 enlisted Marines serving on active duty from 2001 through 2005. The information was being used for a research project on retention of service personnel. Navy officials considered the risk from the breach to be greatly diminished since the thumb drive was lost on a government installation and the drive's data were readable only through software that was password protected and considered in limited distribution.

- The Treasury Inspector General For Tax Administration reported that approximately 490 computers at the Internal Revenue Service (IRS) were

lost or stolen between January 2003, and June 2006. Additionally, 111 incidents occurred within IRS facilities, suggesting that employees were not storing their laptop computers in a secured area while they were away from the office. The IG concluded that it was very likely that a large number of the lost or stolen computers contained unencrypted data and also found other computer devices, such as flash drives, CDs, and DVDs, on which sensitive data were not always encrypted.

- The Department of State experienced a security breach on its unclassified network, which daily processes about 750,000 e-mails and instant messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. The breach involved an e-mail containing what was thought to be an innocuous attachment. However, the e-mail contained code to exploit vulnerabilities in a well-known application for which no security patch existed at that time. Because the vendor was unable to expedite testing and deploy a new patch, the department developed its own temporary fix to protect systems from being exploited further. In addition, the department sanitized the infected computers and servers, rebuilt them, changed passwords, installed critical patches, and updated their antivirus software.

Based on the experience of VA and other federal agencies in responding to data breaches, we identified numerous lessons learned regarding how and when to notify government officials, affected individuals, and the public.[6] As discussed later in this report, OMB has issued guidance that largely addresses these lessons.

Weaknesses Persist at Federal Agencies in Implementing Security Policies and Practices

As illustrated by recent security incidents, significant weaknesses continue 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

[6]GAO, *Privacy: Lessons Learned About Data Breach Notification*, GAO-07-657, (Washington, D.C.: Apr. 30, 2007).

condition[7] or a material weakness (see fig. 2).[8] 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),[9] 17 of 24 agencies reported shortcomings in information security, including 7 that considered it a material weakness. IGs have also noted the seriousness of information security, with 21 of 24 including it as a "major management challenge."[10]

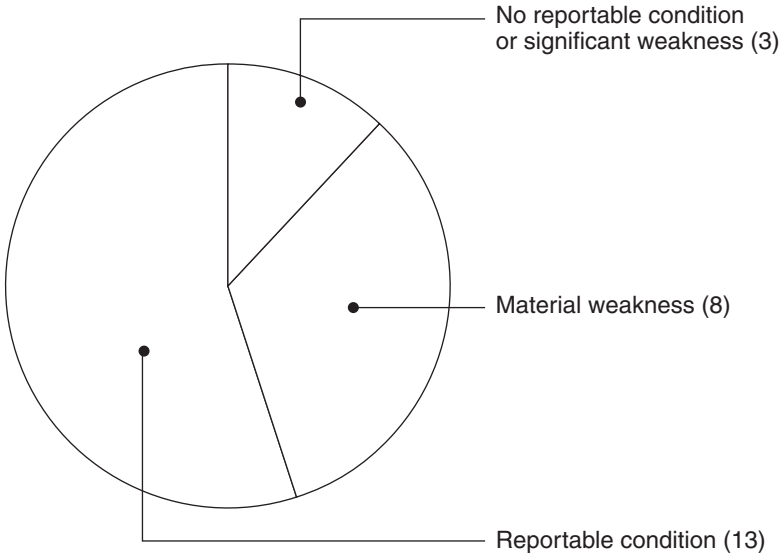
[7]Reportable conditions are significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[8]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.

[9]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.

[10]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.

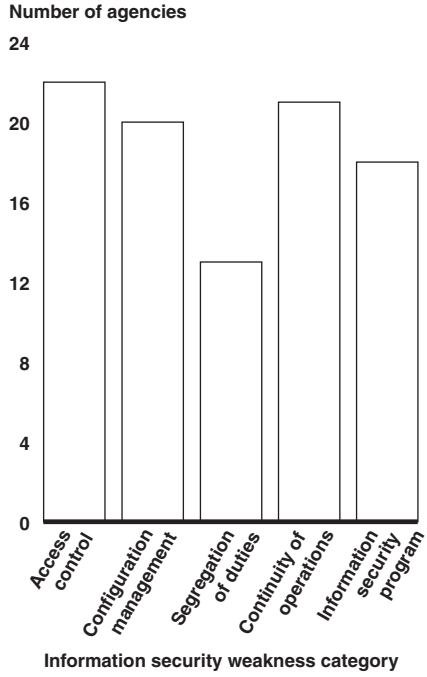
Figure 2: Agencies Reporting of Information Security Controls in Fiscal Year 2006 Financial Statement Audits



Source: GAO analysis of agency financial statement audits.

According to our reports and those of IGs, 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 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 continue to have weaknesses in each of these categories, as shown in figure 3.

Figure 3: Information Security Weaknesses at 24 Major Agencies for Fiscal Year 2006



Source: GAO analysis of IG, agency, and prior GAO reports.

In our prior reports,[11] we have made hundreds of specific recommendations to the agencies to mitigate the weaknesses identified. Similarly, the IGs have issued specific recommendations as part of their information security review work.

Access Controls Were Not Adequate

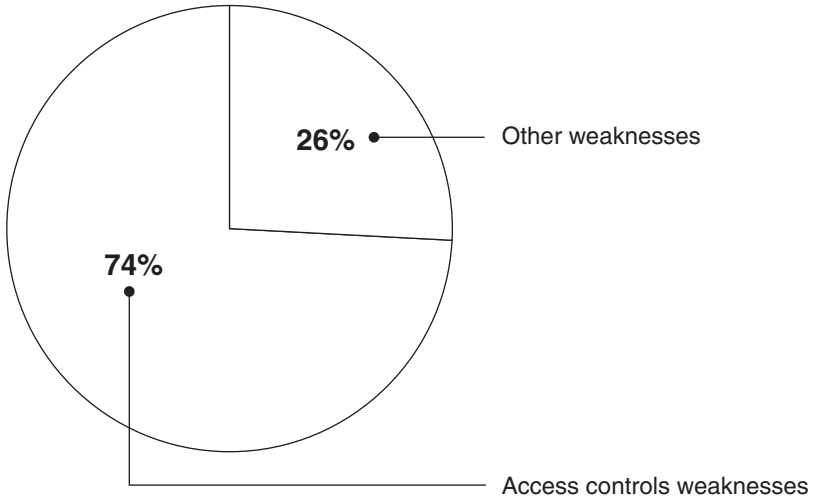
A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Organizations accomplish this task by designing and implementing controls that are intended to prevent, limit, and detect access to computing resources (computers, networks, programs, and data), thereby protecting these resources from unauthorized use, modification, loss, and disclosure. Access controls can be both electronic and physical. Electronic access controls include those related to user identification and

[11]See the Related GAO Products section for a list of our recent reports on information security.

authentication, authorization, boundary protection, cryptography, and audit and monitoring. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which they are housed and enforcing usage restrictions and implementation guidance for portable and mobile devices.

Twenty-two major agencies had access control weaknesses. Analysis of our recent reports have identified that the majority of information security control weaknesses pertained to access controls (see fig. 4). For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply encryption to protect sensitive data on networks and portable devices; and (5) log, audit, and monitor security-relevant events. Agencies also lacked effective controls to restrict physical access to information assets.

Figure 4: Control Weaknesses Identified in GAO Reports From July 2005 to June 2007



Source: GAO analysis of prior GAO reports.

User Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication.

Several agencies have not adequately controlled user accounts and passwords to ensure that only authorized individuals are granted access to its systems and data. For example, several agencies did not always implement strong passwords—using vendor-default or easy-to-guess passwords, or having the minimum password length set to zero. One agency's staff shared logon accounts and passwords when accessing a database production server for the procurement system. By allowing users to share accounts and passwords, individual accountability for authorized system activity as well as unauthorized system activity could be lost. Consequently, users could create short passwords, which tend to be easier to guess or crack than longer passwords. Without appropriate controls over identification and authentication, agencies are at increased risk of unauthorized access.

Authorization

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information. This principle means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those programs and files that they need to do their work, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing users access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions.

Several agencies continued to imprudently grant rights and permissions that allowed more access than users needed to perform their jobs. For example, one agency had granted users of a database system the access rights to create or change sensitive system files—even though they did not have a legitimate business need for this access. Further, the permissions for sensitive system files also inappropriately allowed all users to read, update, or execute them. These types of excessive privileges provide opportunities for individuals to circumvent security controls. In another instance, each user on one organization's network was permitted to have access to sensitive Privacy Act-protected information including names, addresses, and Social Security numbers of individuals. Once a Social Security number is obtained fraudulently, it can then be used to create a false identity for financial misuse, assume another individual's identity, or to fraudulently obtain credit. As a result, there is increased risk that sensitive data and personally identifiable information may be compromised.

Boundary Protection

Boundary protection pertains to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Organizations physically allocate publicly accessible information system components to separate subnetworks with separate physical network interfaces, and they prevent public access into their internal networks. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment.

Several agencies continue to demonstrate vulnerabilities in establishing required boundary protection mechanisms. For example, one agency did not configure a remote access application properly, which permitted simultaneous access to the Internet and the internal network. This could allow an attacker who compromised a remote user's computer to remotely control the user's secure session from the Internet. Another agency failed to ensure that its contractor adequately implemented controls used to protect its external and key internal boundaries. Specifically, certain network devices did not adequately restrict external communication traffic. As a result, an unauthorized individual could exploit these vulnerabilities to launch attacks against other sensitive network devices.

Cryptography

Cryptography[12] underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide 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. The National Security Agency also recommends disabling protocols that do not encrypt information transmitted across the network, such as user identification and password combinations.

Many agencies did not encrypt certain information traversing its networks, but instead used clear text protocols that make network traffic susceptible to eavesdropping. For example, at one agency's field site, all information, including user identification and password information, was being sent across the network in clear text. At another agency, the contractor did not consistently apply encryption to protect network configuration data stored on network devices. These weaknesses could allow an attacker, or malicious user, to view information and use that knowledge to obtain sensitive financial and system data being transmitted over the network.

Audit and Monitoring

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events.

[12]Cryptography is used to secure transactions by providing ways to ensure data confidentiality, data integrity, authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

Agencies did not sufficiently log and monitor key security- and audit-related events. For instance, agencies did not prepare key security reports such as failed login attempt reports. In other cases, logging either was disabled or configured to overwrite, or procedures for classifying and investigating security–related events had not been documented. As a result, unauthorized access could go undetected, and the ability to trace or recreate events in the event of a system modification or disruption could be diminished.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks.

Several agencies also lacked effective physical security controls. Consequently, critical information held by the federal government, such as Social Security numbers or other personal data, can be at acute risk of unnecessary or unauthorized access by individuals intent on perpetrating identity theft and committing financial crimes. For example, one agency granted over 400 individuals unrestricted access to an entire data center—including a sensitive area within the data center—although their job functions did not require them to have such access. In another case, one agency did not adequately protect the entrances to its facilities, as visitor screening procedures were inconsistently implemented and available tools were not being used properly or to their fullest capability. Many of the data losses that occurred at federal agencies over the past few years, discussed earlier in this report, were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Configuration Management Controls Were Not Implemented

Configuration management controls ensure that only authorized and fully tested software is placed in operation. These controls, which also limit and monitor access to powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. These policies, procedures, and techniques help ensure that all programs and program modifications are properly authorized, tested, and approved. Further, patch management is an important element in

mitigating the risks associated with software vulnerabilities. Up-to-date patch installation could help mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage—including the loss of control of entire systems—thereby enabling malicious individuals to read, modify, or delete sensitive information or disrupt operations.

At least 20 major agencies demonstrated weaknesses in configuration management controls. For example, many agencies did not consistently configure network devices and services to prevent unauthorized access and ensure system integrity, such as installing critical software patches in a timely manner. As a result, systems and devices were not updated and were left susceptible to denial-of-service attacks or to malicious users exploiting software vulnerabilities. In light of the recent surge in zero-day exploits, it is imperative for agencies to be prepared for the challenge of testing and deploying patches under a very compressed time frame. Additionally, certain agencies did not implement effective controls to ensure that system software changes were properly authorized, documented, tested, and monitored. Instances also existed where agencies did not maintain current documentation of major modifications to systems or significant changes in processing. Inadequate configuration management controls increases the risk that unauthorized programs or changes could be inadvertently or deliberately placed into operation.

Segregation of Duties Was Not Appropriately Enforced

Segregation of duties refers to the policies, procedures, and organizational structure that helps ensure that one individual cannot independently control all key aspects of a process or computer-related operation and, thereby, conduct unauthorized actions or gain unauthorized access to assets or records. Proper segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. Dividing duties among individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other.

At least 13 agencies did not appropriately segregate information technology duties. These agencies generally did not assign employee duties and responsibilities in a manner that segregated incompatible functions among individuals or groups of individuals. For instance, at one agency, users were allowed to both initiate and authorize the same transaction. At another agency, financial management staff members were permitted to perform both security and systems administration duties for the application, potentially allowing these staff members to conduct fraudulent activity without being detected. Without adequate segregation

of duties, there is an increased risk that erroneous or fraudulent actions can occur, improper program changes implemented, and computer resources damaged or destroyed.

Shortcomings Exist in Continuity of Operations Planning

An organization must take steps to ensure that it is adequately prepared to cope with the loss of operational capabilities due to an act of nature, fire, accident, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity of operations plan. Such a plan should cover all key computer operations and should include planning for business continuity. This plan is essential for helping to ensure that critical information systems, operations, and data such as financial processing and related records can be properly restored if a disaster occurs. To ensure that the plan is complete and fully understood by all key staff, it should be tested—including surprise tests—and test plans and results documented to provide a basis for improvement. If continuity of operations controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.

Although agencies have reported advances in the number of systems for which contingency plans have been tested, at least 21 agencies still demonstrated shortcomings in their continuity of operations planning. For example, one agency did not have a plan that reflected its current operating environment. Another agency had 17 individual disaster recovery plans covering various segments of the organization, but it did not have an overall document that integrated the 17 separate plans and defined the roles and responsibilities for the disaster recovery teams. In another example, the agency had not established an alternate processing site for a key application, or tested the plan. Until agencies complete actions to address these weaknesses, they are at risk of not being able to appropriately recover in a timely manner from certain service disruptions.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented agencywide information security programs. An agencywide security program, required by FISMA, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be

inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

At least 18 of the 24 major federal agencies had not fully or effectively implemented agencywide information security programs. Results of our recent work illustrate that agencies often did not adequately design or effectively implement policies for elements key to an information security program. We identified weaknesses in information security program activities, such as agencies' risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial action plans.

Risk Assessments

Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the adopted policies and controls in order to help ensure their intended operation.

Our evaluations at agencies show that they have not fully implemented risk assessment processes. Furthermore, they did not always effectively evaluate potential risks for the systems we reviewed. For example, one agency had no documented process for conducting risk assessments, while another agency had outdated risk assessments. In another agency, we determined that they had assessed the risk levels for their systems, categorized them on the basis of risk, and had current risk assessments that documented residual risk assessed and potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities they identified. However, that agency did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them. As a result of these weaknesses, inadequate or inappropriate security controls may be implemented that do not address the systems' true risk, and potential risks to these systems may remain unknown.

Policies and Procedures

Although agencies have developed and documented information security policies, standards, and guidelines for information security, they did not always provide specific guidance on how to guard against significant

security weaknesses. For example, policies lacked guidance on how to correctly configure certain identifications used by operating systems and the powerful programs used to control processing. We also found weaknesses in policies regarding physical access, Privacy Act-protected data, wireless configurations, and business impact analyses. As a result, agencies have reduced assurance that their systems and the information they contain are sufficiently protected.

Security Plans

Instances exist where security plans were incomplete or not up-to-date. For example, one agency had systems security plans that were missing required information, such as rules of behavior and controls for public access. At that same agency, one security plan did not identify its system owner. In another instance, requirements for applications were not integrated into the security plan for the general support system, and the interconnectivity of the current system environment was not completely addressed. As a result, agencies' cannot ensure that appropriate controls are in place to protect key systems and critical information.

Specialized Training

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing required training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. However, we identified instances where agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.

System Tests and Evaluations

Agencies' policies and procedures for performing periodic testing and evaluation of information security controls were not always adequate. Our report[13] on testing and evaluating security controls revealed that agencies had not adequately designed and effectively implemented policies for testing their security controls in accordance with OMB and NIST guidance.

[13]GAO, *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

Agencies did not have policies that addressed how to determine the depth and breadth of testing according to risk. Further, agencies did not always address other important elements, such as the definition of roles and responsibilities of personnel performing tests, identification and testing of security controls common to multiple systems, and the frequency of periodic testing. In other cases, agencies had not tested controls for all of their systems. Without appropriate tests and evaluations, agencies have limited assurance that policies and controls are appropriate and working as intended. Additionally, increased risk exists that undetected vulnerabilities could be exploited to allow unauthorized access to sensitive information.

Remedial Action Processes and Plans

Our work uncovered weaknesses in agencies' remediation processes and plans used to document remedial actions. For example, our report[14] on security controls testing revealed that seven agencies did not have policies to describe a process for incorporating weaknesses identified during periodic security control testing into remedial actions. In our other reviews, agencies indicated that they had corrected or mitigated weaknesses; however, we found that those weaknesses still existed. In addition, we reviewed agencies' system self-assessments and identified weaknesses not documented in their remedial action plans. These weaknesses pertained to system audit trails, approval and distribution of continuity of operations plans, and documenting emergency procedures. We also found that some deficiencies had not been corrected in a timely manner. Without a mature process and effective remediation plans, risk increases that vulnerabilities in agencies' systems will not be mitigated in an effective and timely manner.

Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent disruption, unauthorized use, disclosure, and modification. Further, until agencies implement our recommendations to correct specific information security control weaknesses, they remain at increased risk of attack or compromise.

[14]GAO-07-65.

Examples Illustrate Weaknesses at Agencies

Persistent weaknesses are evident in numerous reports. Recent reports by GAO and IGs show that while agencies have made some progress, persistent weaknesses continue to place critical federal operations and assets at risk. In our reports, we have made hundreds of recommendations to agencies to correct specific information security weaknesses. The following examples illustrate the effect of these weaknesses at various agencies and for critical systems.

- Independent external auditors identified over 130 information technology control weaknesses affecting the Department of Homeland Security's (DHS) financial systems during the audit of the department's fiscal year 2006 financial statements. Weaknesses existed in all key general controls and application controls. For example, systems were not certified and accredited in accordance with departmental policy; policies and procedures for incident response were inadequate; background investigations were not properly conducted; and security awareness training did not always comply with departmental requirements. Additionally, users had weak passwords on key servers that process and house DHS financial data, and workstations, servers, and network devices were configured without necessary security patches. Further, changes to sensitive operating system settings were not always documented; individuals were able to perform incompatible duties such as changing, testing, and implementing software; and service continuity plans were not consistently or adequately tested. As a result, material errors in DHS' financial data may not be detected in a timely manner.

- The Department of Health and Human Services (HHS) had not consistently implemented effective electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive financial and medical information at its operating divisions and contractor-owned facilities.[15] Numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events existed in its computer networks and systems. In addition, weaknesses existed in controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. These weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately

[15]GAO, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267 (Washington, D.C.: Feb. 24, 2006).

disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its services.

- The Securities and Exchange Commission had made important progress addressing previously reported information security control weaknesses.[16] However, we identified 15 new information security weaknesses pertaining to the access controls and configuration management existed in addition to 13 previously identified weaknesses that remain unresolved. For example, the Securities and Exchange Commission did not have current documentation on the privileges granted to users of a major application, did not securely configure certain system settings, or did not consistently install all patches to its systems. In addition, the commission did not sufficiently test and evaluate the effectiveness of controls for a major system as required by its certification and accreditation process.

- IRS had made limited progress toward correcting previously reported information security weaknesses at two data processing sites.[17] IRS had not consistently implemented effective access controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. Those access controls included those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. In addition, IRS faces risks to its financial and sensitive taxpayer information due to weaknesses in configuration management, segregation of duties, media destruction and disposal, and personnel security controls.

- The Federal Aviation Administration (FAA) had significant weaknesses in controls that are designed to prevent, limit, and detect access to those systems.[18] For example, for the systems reviewed, the agency was not adequately managing its networks, system patches, user accounts and passwords, or user privileges, and it was not always logging and auditing security-relevant events. In addition, FAA faces risks to its air traffic control systems due to weaknesses in physical security, background investigations, segregation of duties, and application change controls. As a

[16]GAO, *Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission*, GAO-06-256 (Washington, D.C.: Mar. 27, 2007).

[17]GAO, *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service*, GAO-07-364 (Washington, D.C.: Mar. 30, 2007).

[18]GAO, *Information Security: Progress Made, but Federal Aviation Administration Needs to Improve Controls over Air Traffic Control Systems*, GAO-05-712 (Washington, D.C.: Aug. 26, 2005).

result, it was at increased risk of unauthorized system access, possibly disrupting aviation operations. While acknowledging these weaknesses, agency officials stated that because portions of their systems are custom built and use older equipment with special-purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. Nevertheless, the proprietary features of these systems do not protect them from attack by disgruntled current or former employees, who understand these features, or from more sophisticated hackers.

- The Federal Reserve Board (FRB) had not effectively implemented information system controls to protect sensitive data and computing resources for the distributed-based systems and the supporting network environment relevant to Treasury auctions.[19] Specifically, the FRB did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) implement adequate boundary protections to limit connectivity to systems that process Bureau of the Public Debt (BPD) business; (4) apply strong encryption technologies to protect sensitive data in storage and on its networks; (5) log, audit, or monitor security-related events; and (6) maintain secure configurations on servers and workstations. As a result, auction information and computing resources for key distributed-based auction systems that the FRB maintain and operate on behalf of BPD are at an increased risk of unauthorized and possibly undetected use, modification, destruction, and disclosure. Furthermore, other FRB applications that share common network resources with the distributed-based systems may face similar risks.

- Although the Centers for Medicare and Medicaid Services had many information security controls in place that had been designed to safeguard the communication network, key information security controls were either missing or had not always been effectively implemented.[20] For example, the network had control weaknesses in areas such as user identification and authentication, user authorization, system boundary protection, cryptography, and audit and monitoring of security-related events. Taken collectively, these weaknesses place financial and personally identifiable

[19]GAO, *Information Security: Federal Reserve Needs to Address Treasury Auction Systems*, GAO-06-659 (Washington, D.C.: Aug. 30, 2006).

[20]GAO, *Information Security: The Centers for Medicare and Medicaid Services Needs to Improve Controls over Key Communication Network*, GAO-06-750 (Washington, D.C.: Aug. 30, 2006).

medical information transmitted on the network at increased risk of unauthorized disclosure and could result in a disruption in service.

- Certain information security controls over a critical internal Federal Bureau of Investigation (FBI) network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources.[21] Specifically, FBI did not consistently (1) configure network devices and services to prevent unauthorized insider access and ensure system integrity; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Collectively, these weaknesses place sensitive information transmitted on the network at risk of unauthorized disclosure or modification, and could result in a disruption of service, increasing the bureau's vulnerability to insider threats.

Agencies Report Progress, but More Work Is Needed in Implementing Requirements

Federal agencies continue to report steady progress in implementing key information security requirements. Although agencies reported increases in OMB's performance metrics, IGs identified various weaknesses in agencies' implementation of FISMA requirements. Pursuant to its FISMA responsibilities, NIST has continued to issue standards and guidance. Also, agency IGs completed their annual evaluations, although scope and methodologies varied across agencies. Further, OMB expanded its guidance to agencies, with specific emphasis on personally identifiable information and reported to Congress as required. However, opportunities exist to improve reporting.

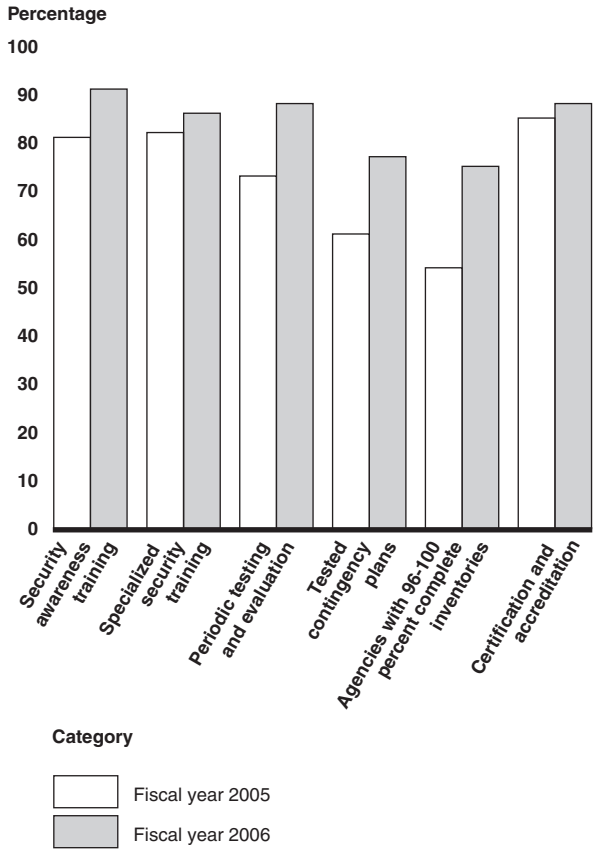
Agencies Cite Increases in Performance, but Weaknesses Exist in FISMA Implementation

For fiscal year 2006 reporting, governmentwide percentages increased for employees and contractors receiving security awareness training and employees with significant security responsibilities receiving specialized training. Percentages also increased for systems that had been tested and evaluated at least annually, systems with tested contingency plans, and systems that had been certified and accredited (see fig. 5). However, IGs at several agencies sometimes disagreed with the information reported by

[21]GAO, *Information Security: FBI Needs to Address Weaknesses in Critical Network*, GAO-07-368 (Washington, D.C.: Apr. 30, 2007).

the agency and have identified weaknesses in the processes used to implement these and other security program activities.

Figure 5: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of IG and agency data.

Security Training and Awareness

Federal agencies rely on their employees to protect the confidentiality, integrity, and availability of the information in their systems. It is critical for each system user to understand their security roles and responsibilities and be adequately trained to perform them. FISMA requires agencies to provide security awareness training to inform personnel—including contractors and other users of information systems that support the operations and assets of the agency—of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide appropriate training on

information security to personnel who have significant security responsibilities. OMB requires agencies to report on the following measures: (1) the number and percentage of employees and contractors who receive information security awareness training, (2) the number and percentage of employees who have significant security responsibilities and received specialized training, (3) whether peer-to-peer file sharing is addressed in security awareness training, and (4) the total amount of money spent on all security training for the fiscal year.

Agencies reported improvements in the governmentwide percentage of employees and contractors receiving security awareness training. According to agency reporting, more than 90 percent of total employees and contractors governmentwide received security awareness training in fiscal year 2006. This is an increase from our 2005 report,[22] in which approximately 81 percent of employees governmentwide received security awareness training. In addition, all agencies reported that they explained policies regarding peer-to-peer file sharing in security awareness training, ethics training, or other agencywide training, all addressed specifically in OMB guidance.

Agencies also reported improvements in the number of employees who had significant security responsibilities and received specialized training. There has been a slight increase in the number of employees who have security responsibilities and received specialized security training since our last report—almost 86 percent of the selected employees had received specialized training in fiscal year 2006, compared with about 82 percent in fiscal year 2005.

To achieve the goal of providing appropriate training to all employees, agencies reported spending an average of $19.28 per employee on security training. The amount of money spent by agencies on security training ranged from about $20,000 to more than $38 million.[23]

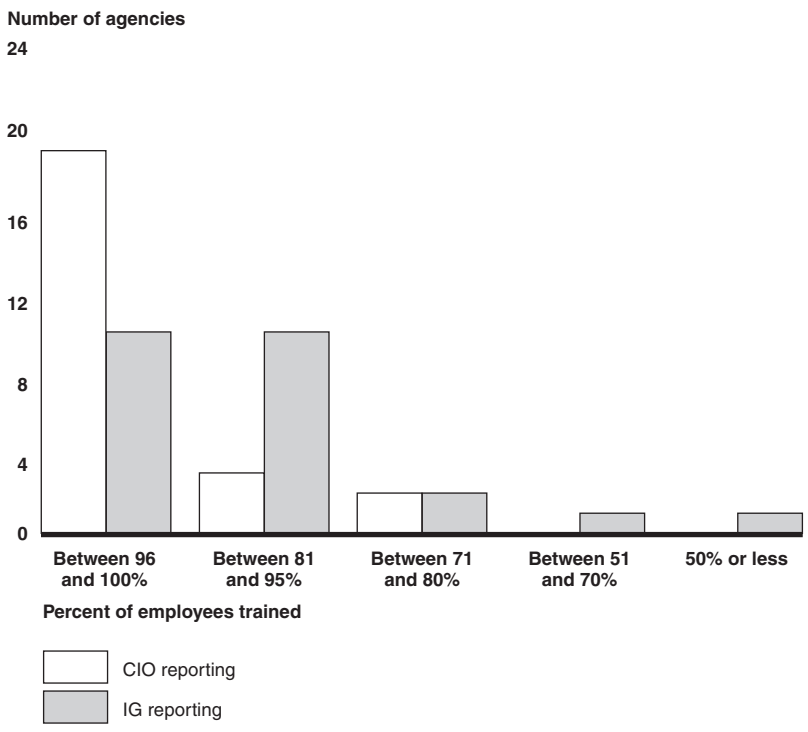
Although agencies have reported improvements in both the number of employees receiving security awareness training and the number of employees who have significant security responsibilities and received

[22]GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[23]One agency did not report the amount of money spent on training.

specialized training, several agencies exhibit training weaknesses. For example, according to agency IGs, five major agencies reported challenges in ensuring that contractors had received security awareness training. In addition, reports from IGs at two major agencies indicated that security training across components was inconsistent. Five agencies also noted that weaknesses still exist in ensuring that all employees who have specialized responsibilities receive specialized training, as policies and procedures for this type of training are not always clear. Further, the majority of agency IGs disagree with their agencies' reporting of individuals who have received security awareness training. Figure 6 shows a comparison between agency and IG reporting of the percentage of employees receiving security awareness training. If all agency employees and contractors do not receive security awareness training, agencies risk security breaches resulting from user error or deliberate attack.

Figure 6: Percentage of Employees Receiving Security Awareness Training As Reported by Agencies and IGs



Source: GAO analysis of agency-reported data.

Periodic Testing and Evaluation of the Effectiveness of Information Security Policies, Procedures, and Practices

Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks proactively, rather than reacting to individual problems ad hoc after a violation has been detected or an audit finding has been reported. Management control testing and evaluation as part of a program review is an additional source of information that can be considered along with controls testing and evaluation in IG and other independent audits to help provide a more complete picture of an agency's security posture. FISMA requires that federal agencies periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of implementing an agencywide security program. This testing is to be performed with a frequency depending on risk, but no less than annually, and consists of testing management, operational, and technical controls for every system identified in the agency's required inventory of major information systems. For annual FISMA reporting, OMB requires that agencies report the number of agency and contractor systems for which security controls have been tested.

In 2006, federal agencies reported testing and evaluating security controls for 88 percent of their systems, up from 73 percent in 2005, including increases in testing high-risk systems. However, shortcomings exist in agencies' testing and evaluation of security controls. For example, the number of agencies testing and evaluating 90 percent or more of their systems decreased from 18 in 2005 to 16 in 2006 reporting. IGs also reported that not all systems had been tested and evaluated at least annually, including some high impact systems, and that weaknesses existed in agencies' monitoring of contractor systems or facilities. As a result, agencies may not have reasonable assurance that controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

Continuity of Operations

Continuity of operations planning ensures that agencies will be able to perform essential functions during any emergency or situation that disrupts normal operations. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, testing contingency plans is essential to determining whether the plans will function as intended in an emergency situation. FISMA requires that agencywide information security programs include plans and procedures to ensure continuity of operations

for information systems that support the operations and assets of the agency. To show the status of implementing contingency plans testing, OMB requires that agencies report the percentage of systems that have contingency plans that have been tested in accordance with policy and guidance.

Federal agencies reported that 77 percent of total systems had contingency plans that had been tested, an increase from 61 percent. However, on average, high-risk systems had the smallest percentage of tested contingency plans—only 64 percent of high-risk systems had tested contingency plans. In contrast, agencies had tested contingency plans for 79 percent of moderate-risk systems, 80 percent of low-risk systems, and 70 percent of uncategorized systems.

Several agencies had specific weaknesses in developing and testing contingency plans. For example, the IG of a major agency noted that contingency planning had not been completed for certain critical systems. Another major agency IG noted that the agency had weaknesses in three out of four tested contingency plans—the plans were inaccurate, incomplete, or outdated, did not meet department and federal requirements, and were not tested in accordance with department and federal government requirements. Without developing contingency plans and ensuring that they are tested, the agency increases its risk that it will not be able to effectively recover and continue operations when an emergency occurs.

Inventory of Systems

A complete and accurate inventory of major information systems is essential for managing information technology resources, including the security of those resources. The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements such as testing systems annually, certifying and accrediting, and testing contingency plans. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. FISMA requires that agencies develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. Beginning with 2005 reporting, OMB no longer required agencies to report the status of their inventories, but required them to report the number of major systems and asked IGs to report on the status and accuracy of their agencies' inventories.

IGs reported that 18 agencies had completed approximately 96-100 percent of their inventories, an increase from 13 agencies in 2005. However, the total number of systems in some agencies' inventories varied widely from 2005 to 2006. In one case, an agency had approximately a 300 percent increase in the number of systems, while another had approximately a 50 percent reduction in the number of its systems. IGs identified problems with agencies' inventories. For example, IGs at two large agencies reported that their agencies still did not have complete inventories, while another questioned the reliability of its agency's inventory since that agency relied on its components to report the number of systems and did not validate the numbers. Without complete, accurate inventories, agencies cannot effectively maintain and secure their systems. In addition, the performance measures used to assess agencies' progress may not accurately reflect the extent to which these security practices have been implemented.

Certification and Accreditation

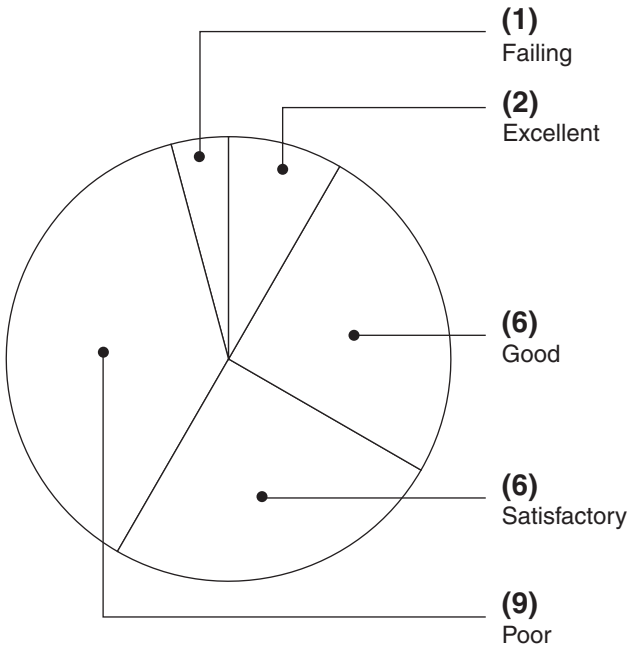
As a key element of agencies' implementation of FISMA requirements, OMB has continued to emphasize its long-standing policy of requiring a management official to formally authorize (or accredit) an information system to process information and accept the risk associated with its operation based on a formal evaluation (or certification) of the system's security controls. For annual reporting, OMB requires agencies to report the number of systems, including impact levels, authorized for processing after completing certification and accreditation. OMB's FISMA reporting instructions also requested IGs to assess and report on their agencies' certification and accreditation process.

Federal agencies continue to report increasing certification and accreditation from fiscal year 2005 reporting. For fiscal year 2006, 88 percent of agencies' systems governmentwide were reported as certified and accredited, as compared with 85 percent in 2005. In addition, 23 agencies reported certifying and accrediting more than 75 percent of their systems, an increase from 21 agencies in 2005. However, the certification and accreditation percentage for uncategorized systems exceeded the percentages for all other impact categories and indicates that agencies may not be focusing their efforts properly.

Although agencies reported increases in the overall percentage of systems certified and accredited, results of work by their IGs showed that agencies continue to experience weaknesses in the quality of this metric. As figure 7 depicts, 10 IGs rated their agencies' certification and accreditation process as poor or failing, while in 2005, 7 IGs rated their agencies' process as poor, and none rated it as failing. In at least three instances of agencies

reporting certification and accreditation percentages over 90 percent, their IG reported that the process was poor. Moreover, IGs continue to identify specific weaknesses with key documents in the certification and accreditation process such as risk assessments and security plans not being completed consistent with NIST guidance or finding those items missing from certification and accreditation packages. In other cases, systems were certified and accredited, but controls or contingency plans were not properly tested. For example, IG reports highlighted weaknesses in security plans such as agencies not using NIST guidance, not identifying controls that were in place, not including minimum controls, and not updating plans to reflect current conditions. Because of these discrepancies and weaknesses, reported certification and accreditation progress may not be providing an accurate reflection of the actual status of agencies' implementation of this requirement. Furthermore, agencies may not have assurance that accredited systems have controls in place that properly protect those systems.

Figure 7: OIG Assessment of C&A Process for Fiscal Year 2006



Source: GAO analysis of IG assessments.

Configuration Standards

Risk-based policies and procedures 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 in their information security program; a key aspect of these policies and procedures is minimally acceptable configuration standards. Configuration standards minimize the security risks associated with specific software applications widely used in an agency or across agencies. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, making the many products vulnerable before they are used.

FISMA requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In fiscal year 2004, for the first time, agencies reported on the degree to which they had implemented security configurations for specific operating systems and software applications. For annual FISMA reporting, OMB requires agencies to report whether they have an agencywide security configuration policy; what products, running on agency systems, are covered by that policy; and to what extent the agency has implemented policies for those products. OMB also requested IGs to report this performance for their agencies.

Agencies had not always implemented security configuration policies. Twenty-three of the major federal agencies reported that they currently had an agencywide security configuration policy. Although 21 IGs agreed that their agency had such a policy, they did not agree that the implementation was always as high as agencies reported. To illustrate, one agency reported implementing configuration policy for a particular platform 96 to 100 percent of the time, while their IG reported that the agency implemented that policy only 0 to 50 percent of the time. One IG noted that three of the agency's components did not have overall configuration policies and that other components that did have the policies did not take into account applicable platforms. If minimally acceptable configuration requirements policies are not properly implemented and applied to systems, agencies will not have assurance that products are configured adequately to protect those systems, which could increase their vulnerability and make them easier to compromise.

Security Incident Procedures

Although strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an organization to improve its understanding of threats

and potential cost of security incidents, as well as pinpointing vulnerabilities that need to be addressed so that they are not exploited again. When incidents occur, agencies are to notify the federal information security incident center—U. S. Computer Emergency Readiness Team (US-CERT). US-CERT uses NIST's definition of an incident (a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices)." The categories defined by NIST and US-CERT are:

- *Unauthorized access*: In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.

- *Denial of service*: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.

- *Malicious code*: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.

- *Improper usage*: A person violates acceptable computing use policies.

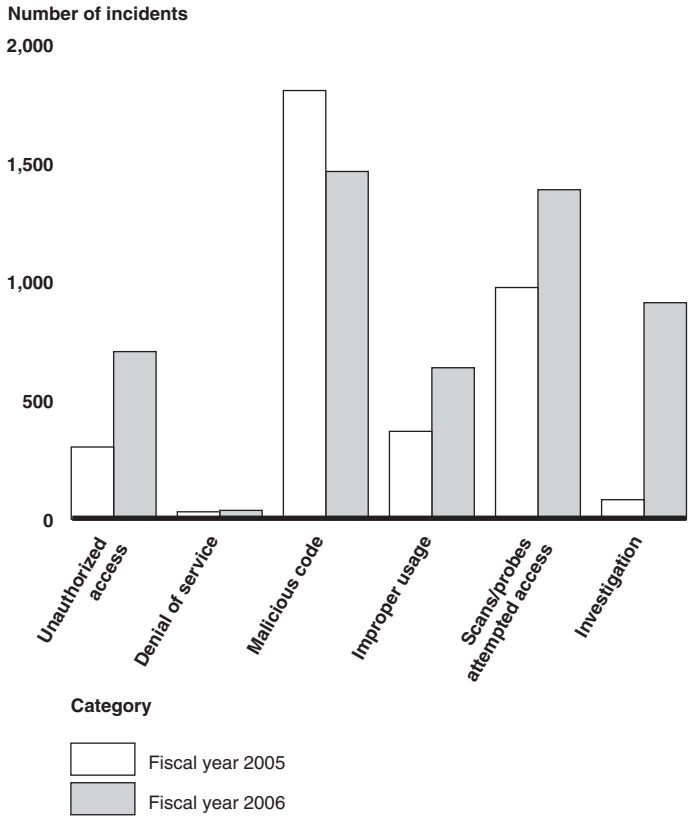
- *Scans/probes/attempted access*: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.

- *Investigation*: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

FISMA requires that agencies' security programs include procedures for detecting, reporting, and responding to security incidents. NIST states that agencies are responsible for determining specific ways to meet these requirements. For FISMA reporting, OMB requires agencies to report numbers of incidents for the past fiscal year in addition to the number of incidents the agency reported to US-CERT and the number reported to law enforcement.

According to the US-CERT annual report for fiscal year 2006, federal agencies reported a record number of incidents, with a notable increase in incidents reported in the second half of the year. As figure 8 shows, since 2005, the number of incidents reported to US-CERT increased in every category except for malicious code.

Figure 8: Incidents Reported to US-CERT in Fiscal Years 2005 and 2006



Source: GAO analysis of OMB data.

Although agencies reported a record number of incidents, shortcomings exist in agencies' security incident reporting procedures. The number of incidents reported is likely to be inaccurate because of inconsistencies in reporting at various levels. For example, one agency reported no incidents to US-CERT, although it reported more than 800 unsuccessful incidents internally and to law enforcement authorities. In addition, analysis of reports from three agencies indicated that procedures for reporting incidents locally were not followed—two where procedures for reporting

incidents to law enforcement authorities were not followed, and one where procedures for reporting incidents to US-CERT were not followed. Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably, information being omitted from incident reports, and reporting time requirements not being met. Without properly accounting for and analyzing security problems and incidents, agencies risk losing valuable information needed to prevent future exploits and understand the nature and cost of threats directed at the agency.

Remedial Actions to Address Deficiencies in Information Security Policies, Procedures, and Practices

Developing remedial action plans is key to ensuring that remedial actions are taken to address significant deficiencies and reduce or eliminate known vulnerabilities. These plans should list the weaknesses and show the estimated resource needs and the status of corrective actions. The plans are intended to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. FISMA requires that agency information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices. For annual FISMA reporting, OMB requires agencies to report quarterly performance regarding their remediation efforts for all programs and systems where a security weakness has been identified. It also requested that IGs assess and report on whether their agency has developed, implemented, and managed an agencywide process for these plans.

IGs reported weaknesses in their agency's remediation process. According to IG assessments, 16 of the 24 major agencies did not almost always incorporate information security weaknesses for all systems into their remediation plans. They found that vulnerabilities from reviews were not always being included in remedial actions. They also highlighted other weaknesses that included one agency having an unreliable process for prioritizing weaknesses and another using inconsistent criteria for defining weaknesses to include in those plans. Without a sound remediation process, agencies cannot be assured that information security weaknesses are efficiently and effectively corrected.

NIST Fulfills FISMA Requirements and Expands Activities

NIST plays a key role under FISMA in providing important standards and guidance. It is required, among other things, to develop and issue minimum information security standards. NIST has issued guidance through its FISMA Implementation Project and has also expanded its work through other security activities.

FISMA Implementation Project

After FISMA was enacted, NIST developed the FISMA Implementation Project to enable it to fulfill its statutory requirements in a timely manner. This project is divided into three phases. Phase I focuses on the development of a suite of required security standards and guidelines as well as other FISMA-related publications necessary to create a robust information security program and effectively manage risk to agency operations and assets. Standards and guidance issued during Phase I included standards for security categorization of federal information and information systems, minimum security requirements for federal information and information systems, and guidance for the recommended security controls for federal information systems. Phase I is nearly complete, with only one publication—a guide to assessing information security controls—remaining to be finalized.

NIST has also developed many other documents to assist information security professionals. For example, NIST issued *Special Publication 800-80* to assist agencies in developing and implementing information security metrics.[24] The processes and methodologies described link information security performance to agency performance by leveraging agency-level strategic planning processes. Additionally, in October 2006, NIST published *Special Publication 800-100*, which provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.[25]

Phase II focuses on the development of a program for accrediting public and private sector organizations to conduct security certification services for federal agencies as part of agencies' certification and accreditation requirements. Organizations that participate in the organizational accreditation program[26] can demonstrate competency in the application of NIST security standards and guidelines. NIST conducted a workshop on

[24]NIST, *Guide for Developing Performance Metrics for Information Security* , SP 800-80 (Washington, D.C.: May 2006)

[25]NIST, *Information Security Handbook: A Guide for Managers*, SP 800-100 (Washington, D.C.: October 2006)

[26]The term accreditation is used in two different contexts in the FISMA Implementation Project: security accreditation is the official management decision to authorize the operation of an information system (as in the certification and accreditation process) and organizational accreditation involves comprehensive proficiency testing and the demonstration of specialized skills in a particular area of interest.

Phase II implementation in April of 2006. It is scheduled to be completed in 2008.

Phase III is the development of a program for validating security tools. The program is to rely on private sector, accredited testing laboratories to conduct evaluations of the security tools. NIST is to provide validation services and laboratory oversight. Implementation of this phase is planned for 2007 and 2008.

Other NIST Security Activities

In addition to the specific responsibilities to develop standards and guidance, other information security activities undertaken by NIST include:

- conducting workshops on the credentialing program for security assessment service providers,
- conducting a presentation on automated security tools,
- providing a tutorial on security certification and accreditation of federal information systems,
- developing and maintaining a checklist repository of security configurations for specific IT products,
- developing, along with other federal agencies, the National Vulnerability Database, which includes a repository of standards based vulnerability management data as well as the security controls, control enhancements, and supplemental guidance from NIST *Special Publication 800-53*,[27] and
- issuance of the Computer Security Division's 2006 *Annual Report* as mandated by FISMA.

Through NIST's efforts in standards and guidance development and other activities, agencies have access to additional tools that can be applied to improve their information security programs. Additionally, NIST's activities will provide federal agencies with opportunities to utilize private-sector resources in improving information security.

[27]NIST, *Recommended Security Controls for Federal Information Systems*, NIST SP 800-53 rev.1 (Washington, D.C.: December 2006)

Office of Inspector General Evaluations Varied across Agencies

FISMA requires agency IGs to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of such programs and practices. Each evaluation is to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assessing compliance (based on the results of the testing) with FISMA requirements and related information security policies, procedures, standards, and guidelines. These required evaluations are then submitted by each agency to OMB in the form of a template. In addition to the template submission, OMB encourages the IGs to provide any additional narrative in an appendix to the report to the extent they provide meaningful insight into the status of the agency's security or privacy program.

Although the IGs conducted annual evaluations, the scope and methodology of IGs' evaluations varied across agencies. For example,

- According to their FISMA reports, certain IGs reported interviewing officials and reviewing agency documentation, while others indicated conducting tests of implementation plans (e.g. security plans).
- Mutiple IGs indicated in their scope and methodology sections of their reports that their reviews were focused on selected components, whereas others did not make any reference to the breadth of their review.
- Several reports were solely comprised of a summary of relevant information security audits conducted during the fiscal year, while others included additional evaluation that addressed specific FISMA-required elements, such as risk assessments and remedial actions.
- The percentage of systems reviewed varied; 22 of 24 IGs tested the information security program effectiveness on a subset of systems; two IGs did not review any systems.
- One IG noted missing Web applications and concluded that the agency's inventory of major systems was only 0 to 50 percent complete, although it noted that, due to time constraints, it was unable to determine whether other items were missing.
- One IG office noted that although it had evaluated the agency's configuration policy and certain aspects of the policy's implementation, it did not corroborate the use of systems under configuration management.

The IG did not independently corroborate whether agency systems ran the software, but instead reflected the agency's response.

- Some reviews were limited due to difficulties in verifying information provided to them by agencies. Specifically, certain IGs stated that they were unable to conduct evaluations of their respective agency's inventory because the information provided to them by the agency at that time was insufficient (i.e., incomplete or unavailable).

The lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content.

The President's Council on Integrity and Efficiency (PCIE)[28] has recognized the importance of having a framework and in September 2006 developed a tool to assist the IG community with conducting its FISMA evaluations. The framework consists of program and system control areas that map directly to the control areas identified in NIST *Special Publication 800-100*[29] and NIST *Special Publication 800-53*,[30] respectively. According to PCIE members, the framework includes broad recommendations rather than a specific methodology due to the varying levels of resources available to each agency IG. This framework could provide a common approach to completing the required evaluations, and PCIE has encouraged IGs to use it.

OMB Increases Guidance, but Improvements Needed in Reporting

Although OMB has continued to expand its guidance provided to agencies to help improve information security at agencies, shortcomings exist in its reporting instructions.

OMB Increases Oversight Efforts

FISMA specifies that, among other responsibilities, OMB is to develop policies, principles, standards and guidelines on information security. Each year, OMB provides instructions to federal agencies and their IGs for FISMA annual reporting. OMB's reporting instructions focus on

[28]The President's Council on Integrity and Efficiency was established by executive order to address integrity, economy, and effectiveness issues that transcend individual government agencies and increase the professionalism and effectiveness of IG personnel throughout government.

[29]SP 800-100.

[30]SP 800-53 rev. 1.

performance measures such as certification and accreditation, testing of security controls, and security training.

In its March 2007 report to Congress on fiscal year 2006 FISMA implementation, OMB noted the federal government's modest progress in meeting key performance measures for IT security. In its report, OMB stressed that there are still areas requiring strategic and continued management attention.

OMB identified progress in the following areas:

- system certification and accreditation,
- testing of security controls and contingency plans,
- assigning risk levels to systems,
- training employees in security, and
- reporting incidents.

OMB indicated the following areas require continued management attention:

- the quality of certification and accreditations,
- inventory of systems,
- oversight of contractor systems, and
- agencywide plan of action and milestones process.

The OMB report also discusses a plan of action to improve performance, assist agencies in their information security activities, and promote compliance with statutory and policy requirements.

To help agencies protect sensitive data from security incidents, OMB has issued several policy memorandums over the past 13 months. For example, OMB has sent memorandums to agencies to reemphasize their responsibilities under law and policy to (1) appropriately safeguard sensitive and personally identifiable information, (2) train employees on their responsibilities to protect sensitive information, and (3) report security incidents. In May 2007, OMB issued additional detailed guidelines

to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, and developing and implementing a policy outlining the rules of behavior, as well as identifying consequences and potential corrective actions for failure to follow these rules.

OMB also issued a memorandum to agencies concerning adherence to specific configuration standards for Windows Vista and XP operating systems. This memorandum requires agencies, with these operating systems and/or plans of upgrading to these operating systems, to adopt the standard security configurations (developed through consensus among DHS, NIST, and the Department of Defense) by February 1, 2008. Agencies were also required to provide OMB with their implementation plans for these platforms by May 1, 2007.

Opportunities Exist to Improve FISMA Reporting

Periodic reporting of performance measures for FISMA requirements and related analysis provides valuable information on the status and progress of agency efforts to implement effective security management programs; however, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. In response, OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. OMB has also recognized the need for assurance of quality for agency processes. For example, OMB specifically requested that the IGs evaluate the certification and accreditation process. The qualitative assessments of the process allow the IG to rate its agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing."

Despite these enhancements, the current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality of agencies' test and evaluation processes. Similarly, OMB's

reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, or incident reporting. Providing information on the quality of the processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

Further, OMB reporting guidance and performance measures do not include complete reporting on a key FISMA-related activity. FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. As we previously reported, maintaining up-to-date patches is key to complying with this requirement. As such, we recommended that OMB address patch management in its FISMA reporting instructions. Although OMB addressed patch management in its 2004 FISMA reporting instructions, it no longer requests this information. Our recent reports have identified weaknesses in agencies' patch management processes, leaving federal information systems exposed to vulnerabilities associated with flaws in software code that could be exploited to cause significant damage—including the loss of control of entire systems—thereby enabling malicious individuals to read, modify, or delete sensitive information or disrupt operations. Without information on agencies' patch management processes, OMB and the Congress lack information that could demonstrate whether or not agencies are taking appropriate steps for protecting their systems.

Conclusions

Persistent governmentwide weaknesses in information security controls threaten the confidentiality, integrity, and availability of the sensitive data maintained by federal agencies. Weaknesses exist predominantly in access controls, including authentication and identification, authorization, cryptography, audit and monitoring, boundary protection, and physical security. Weaknesses also exist in configuration management, segregation of duties and continuity of operations. Until agencies ensure that their information security programs are fully and effectively implemented, there is limited assurance that sensitive data will be adequately protected against unauthorized disclosure or modification or that services will not be interrupted. These weaknesses leave federal agencies vulnerable to external as well as internal threats. Until agencies fully and effectively implement their information security programs, including addressing the hundreds of recommendations that we and IGs have made, federal systems will remain at increased risk of attack or compromise.

Despite federal agencies' reported progress and increased activities, weaknesses remain in the processes agencies use for implementing FISMA performance measures such as those related to agency risk management. In addition, NIST, the IGs, and OMB have all made progress toward fulfilling their requirements. However, the metrics specified in current reporting guidance do not measure how effectively agencies are performing various activities and the guidance does not address a key activity. The absence of this information could result in reporting that does not adequately reflect the status of agency implementation of required information security policies and procedures. Subsequently, oversight entities may not be receiving information critical for monitoring agency compliance with FISMA's statutory requirements for an information security program.

Recommendations for Executive Action

Because annual reporting is critical to monitoring agencies' implementation of information security requirements, we recommend that the Director of OMB take the following three actions in revising future FISMA reporting guidance:

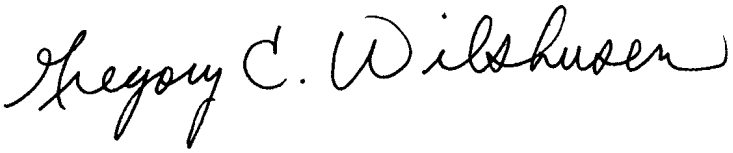
- Develop additional performance metrics that measure the effectiveness of FISMA activities.
- Request inspectors general to report on the quality of additional agency information security processes, such as system test and evaluation, risk categorization, security awareness training, and incident reporting.
- Require agencies to report on a key activity—patch management.

Agency Comments

We received written comments on a draft of this report from the Administrator, Office of E-Government and Information Technology, OMB (see app. II). The Administrator agreed to take our recommendations under advisement when the Office modifies its FISMA reporting instructions. In addition, the Administrator pointed out that the certification and accreditation process provides a systemic approach for determining whether appropriate security controls are in place, functioning properly, and producing the desired outcome. She further noted that OMB's current instructions for IGs to evaluate the quality of agencies' certification and accreditation process provide the flexibility for IGs to tailor their evaluations based on documented weaknesses and plans for improvement.

We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform and to the Office of Management and Budget. We will also make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

In accordance with the Federal Information Security Management Act of 2002 (FISMA) requirement that the Comptroller General report periodically to Congress, our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agency implementation of FISMA requirements.

To assess the adequacy and effectiveness of agency information security policies and practices, we analyzed our related reports issued from May 2005 through May 2007. We also reviewed and analyzed the information security work and products of the agency inspectors general. Both our reports and the Inspector(s) General products generally used the methodology contained in *The Federal Information System Controls Audit Manual*. Further, we reviewed and analyzed data on information security in federal agencies' performance and accountability reports.

To assess implementation of FISMA requirements, we reviewed and analyzed the act (Title III, Pub. L. No. 107-347) and the 24 major federal agencies' chief information officer and IG FISMA reports for fiscal years 2004 to 2006, as well as the performance and accountability reports for those agencies; the Office of Management and Budget's FISMA reporting instructions, mandated annual reports to Congress, and other guidance; and the National Institute of Standards and Technology's standards, guidance, and annual reports. We also held discussions with agency officials and the agency inspectors general to further assess the implementation of FISMA requirements. We did not include systems categorized as national security systems in our review, nor did we review the adequacy or effectiveness of the security policies and practices for those systems.

Our work was conducted in Washington, D.C. from February 2007 through June 2007 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Office of Management and Budget

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

JUL 17 2007

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office

Dear Mr. Wilshusen,

Thank you for the opportunity to comment on the draft Government Accountability Office's (GAO's) report titled, "Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses" (GAO-07-837). We appreciate GAO's careful review and interest in improving agency security programs and agree that progress has been reported.

In the draft report, GAO recommends that the Office of Management and Budget (OMB) take the following three actions in revising future Federal Information Security Management Act (FISMA) reporting guidance:

- Develop additional performance metrics that measure the effectiveness of FISMA activities.
- Request inspectors general to report on the quality of additional information security processes, such as system test and evaluation, risk categorization, security awareness training, and incident reporting.
- Request agencies to report on a key activity, specifically patch management.

Since 2004, OMB has instructed inspectors general to evaluate the quality of the agency certification and accreditation (C&A) process. While no process will guarantee a secure system, C&A provides a systematic approach for determining whether appropriate security controls are in place, functioning properly, and producing the desired outcome. It also provides authorizing officials with the information needed to make informed decisions based on knowledge of the remaining risks.

The C&A process requires agencies to categorize systems by impact and risk level, identify adequate controls commensurate with the impact level and risk, and test the effectiveness of all technical, operational, and management controls (e.g., reporting incidents, providing security awareness training, and applying patches) used to adequately secure each system and as outlined in NIST Special Publication 800-53, "Recommended Security Controls for Information Systems" found at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

By instructing agencies to qualitatively review agency C&A processes, OMB ensures agencies and their inspectors general have the flexibility provided by FISMA (see section

3545(a) and section 3545(a)(2)(A) of FISMA) to tailor their evaluations based on the agency's documented weaknesses and plans for improvement. This ensures evaluations by inspectors general include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.

If OMB were to request quality reviews on specific control groups, we would require qualitative reviews on certain areas where agencies may already be effective. We would also reduce the flexibility needed by agencies to tailor their evaluations to address documented weaknesses at their agency. As a result, OMB would place agencies at risk of not reviewing controls needing improvement.

Nonetheless, GAO's recommendation, in principle, is consistent with FISMA and OMB guidance, inasmuch as it encourages agencies to review the quality of their security processes. As such, we will take GAO's recommendations under advisement when we modify our FISMA reporting instructions.

Thank you again for the opportunity to review and provide comment on your draft report.

Sincerely,

Karen S. Evans
Administrator
Office of E-Government and IT

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244
Director, Information Security Issues

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director); Eric Costello; Larry Crosland; Nancy Glover; Min Hyun; and Jayne Wilson made key contributions to this report.

Related GAO Products

Information Security: FBI Needs to Address Weaknesses in Critical Network. GAO-07-368. Washington, D.C.: April 30, 2007.

Information Security: Persistent Weaknesses Highlight Need for Further Improvement. GAO-07-751T. Washington, D.C.: April 19, 2007.

Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service. GAO-07-364. Washington, D.C.: March 30, 2007.

Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission. GAO-07-256. Washington, D.C.: March 27, 2007.

Information Security: Veterans Affairs Needs to Address Long-Standing Weaknesses. GAO-07-532T. Washington, D.C.: February 28, 2007.

Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing. GAO-07-65. Washington, D.C.: October 20, 2006.

Information Security: Coordination of Federal Cyber Security Research and Development. GAO-06-811. Washington, D.C.: September 29, 2006.

Information Security: Federal Deposit Insurance Corporation Needs to Improve Its Program. GAO-06-620. Washington, D.C.: August 31, 2006.

Information Security: Federal Reserve Needs to Address Treasury Auction Systems. GAO-06-659. Washington, D.C.: August 30, 2006.

Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network. GAO-06-750. Washington, D.C.: August 30, 2006.

Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs. GAO-06-897T. Washington, D.C.: June 20, 2006.

Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues. GAO-06-866T. Washington, D.C.: June 14, 2006.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. GAO-06-408. Washington, D.C.: March 31, 2006.

Information Assurance: National Partnership Offers Benefits, but Faces Considerable Challenges. GAO-06-392. Washington, D.C.: March 24, 2006.

Information Security: Continued Progress Needed to Strengthen Controls at the Internal Revenue Service. GAO-06-328. Washington, D.C.: March 23, 2006.

Bureau of the Public Debt: Areas for Improvement in Information Security Controls. GAO-06-522R. Washington, D.C.: March 16, 2006.

Information Security: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements. GAO-06-527T. Washington, D.C.: March 16, 2006.

Information Security: Department of Health and Human Services Needs to Fully Implement Its Program. GAO-06-267. Washington, D.C.: February 24, 2006.

Information Security: The Defense Logistics Agency Needs to Fully Implement Its Security Program. GAO-06-31. Washington, D.C.: October 7, 2005.

Information Security: Progress Made, but Federal Aviation Administration Needs to Improve Controls over Air Traffic Control Systems. GAO-05-712. Washington, D.C.: August 26, 2005.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO-05-552. Washington, D.C.: July 15, 2005.

Information Security: Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology. GAO-05-849T. Washington, D.C.: June 22, 2005.

Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program. GAO-05-700. Washington, D.C.: June 17, 2005.

Information Security: Radio Frequency Identification Technology in the Federal Government. GAO-05-551. Washington, D.C.: May 27, 2005.

IRS Modernization: Continued Progress Requires Addressing Resource Management Challenges. GAO-05-707T. Washington, D.C.: May 19, 2005.

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 "Subscribe to 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, 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

Congressional Relations

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

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548