United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Oversight and Government Reform
House of Representatives

For Release on Delivery
Expected at 2:00 pm EDT
Thursday, June 7, 2007

INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-07-935T

June 7, 2007

INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-935T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

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.

In this testimony, GAO discusses security incidents reported at federal agencies, the continued weaknesses in information security controls at major federal agencies, agencies' progress in performing key control activities, and opportunities to enhance FISMA reporting and independent evaluations. To address these objectives, GAO analyzed agency, inspectors general (IG), and GAO issued and draft reports on information security.

www.gao.gov/cgi-bin/getrpt?GAO-07-935T.

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

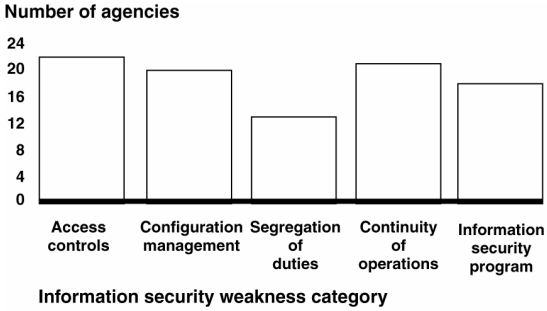
What GAO Found

Federal agencies have recently reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscore the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. 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 networks, systems, or information. For example, agencies did not consistently identify and authenticate users to prevent unauthorized access, apply encryption to protect sensitive data on networks and portable devices, and restrict physical access to information assets. 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; 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.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. However, IGs at several agencies sometimes disagreed with the agency's reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis.

Mr. Chairmen and Members of the Subcommittees:

Thank you for the opportunity to participate in today's joint hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Proper safeguards are essential to protect systems from malicious insiders and external attackers attempting to gain unauthorized access and obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. Over the past year, federal agencies have reported numerous security incidents.

For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences. In reports to Congress since 1997, we have identified information security as a governmentwide high-risk issue.[1] Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[2] which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

In my testimony today, I will summarize (1) security incidents reported at federal agencies, (2) the effectiveness of information security at federal agencies, (3) agencies' reported progress in performing key control activities, and (4) opportunities to enhance FISMA reporting and independent evaluations. In preparing for this testimony, we relied on our previous reports and ongoing work on information security at federal agencies. We also analyzed agencies'

[1]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

inspectors general (IG) reports pertaining to information security; congressional reports; annual FISMA reports for 24 major federal agencies;[3] the performance and accountability reports for those agencies; and the Office of Management and Budget (OMB) FISMA guidance and mandated annual reports to Congress. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Recently reported information security incidents at federal agencies have placed sensitive data at risk. For example, personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscores the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all of the 24 major federal agencies had weaknesses in 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

[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.

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 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; 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 disruption, attack, or compromise.

Despite persistent information security weaknesses, federal agencies have continued to report steady progress in implementing certain information security requirements. 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.[4] However, IGs at several agencies sometimes disagreed with the agency reported information and identified weaknesses in the processes used to implement these and other security program activities.

Opportunities exist for enhanced FISMA reporting and independent evaluations. Although OMB increased its reporting guidance to agencies, the metrics used do not measure how effectively agencies

[4]OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

are performing various activities. For example, agencies report on the number of systems undergoing test and evaluation in the past year, but there is no measure of the quality of agencies' test and evaluation processes. Additionally, there are no requirements to report on certain key activities such as patch management. Further, independent annual evaluations completed by IGs lack a common approach. The scope and methodologies used by IGs varied across agencies, resulting in the collective IG community performing their evaluations without optimal effectiveness and efficiency. A common framework may provide IGs with the means to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently.

Background

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. Hence, the degree of risk caused by security weaknesses is high. For example, resources (such as federal payments and collections) could be lost or stolen, data could be modified or destroyed, and 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 improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services. Finally, agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Recognizing the importance of securing federal systems and data, Congress passed FISMA, which sets forth a comprehensive framework for ensuring the effectiveness of 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 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. More specifically, FISMA requires agency information security programs that, among other things, include

- periodic assessments of the risk;
- risk-based policies and procedures;
- 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;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

In addition, agencies must develop and maintain an inventory of major information systems that is updated at least annually.

OMB and agency IGs play key roles under FISMA. FISMA specifies that, among other responsibilities, OMB is to develop policies, principles, standards, and guidelines on information security, and is required to report annually to Congress. OMB has provided instructions to federal agencies and their IGs for FISMA annual reporting. OMB's reporting instructions focus on performance metrics such as certification and accreditation, testing of security

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

controls, and security training. Its yearly guidance also requests IGs to report on their agencies' efforts to complete their inventory of systems and requires agencies to identify any physical or electronic incidents involving the loss of, or unauthorized access to, personally identifiable information.

FISMA also 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 that summarizes the results. In addition to the template submission, OMB encourages the IGs to provide any additional narrative in an appendix to the report that provides meaningful insight into the status of the agency's security or privacy program.

Incidents Place Sensitive Information at Risk

Since May 2006, federal agencies have reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. 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 concerning steps 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 & 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 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 those who may have been affected.
- 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.
- 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 were unable to clearly define the amount of time that perpetrators were

inside its computers, or find any evidence to show that data was lost as a result.

- 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 the employees 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 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 further exploited. In addition, the department sanitized the infected computers and servers, rebuilt them, changed all passwords, installed critical patches, and updated their anti-virus 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] These lessons have largely been addressed in guidance issued by OMB. OMB has issued several policy memorandums over the past 13 months. For example, it 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

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

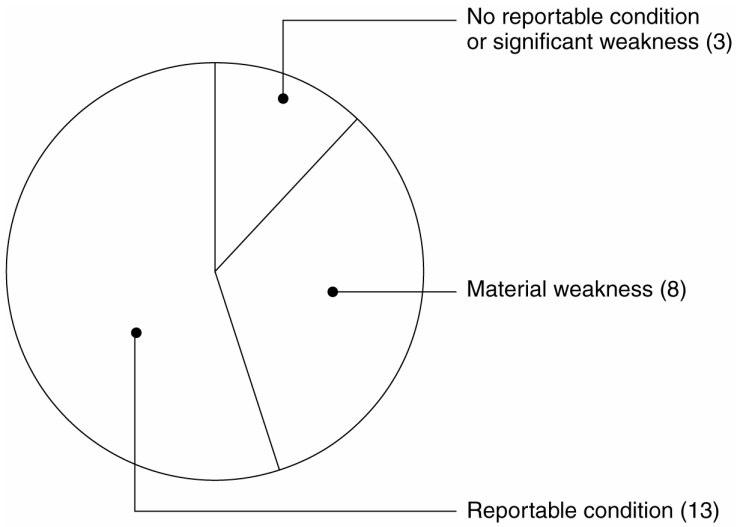
guidelines to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, 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.

Weaknesses Persist at Federal Agencies

As illustrated by numerous 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 condition or material weakness (see fig. 1).[7] Our audits continue to identify similar conditions in both financial and non-financial systems, including agencywide weaknesses as well as weaknesses in critical federal systems.

[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. 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.

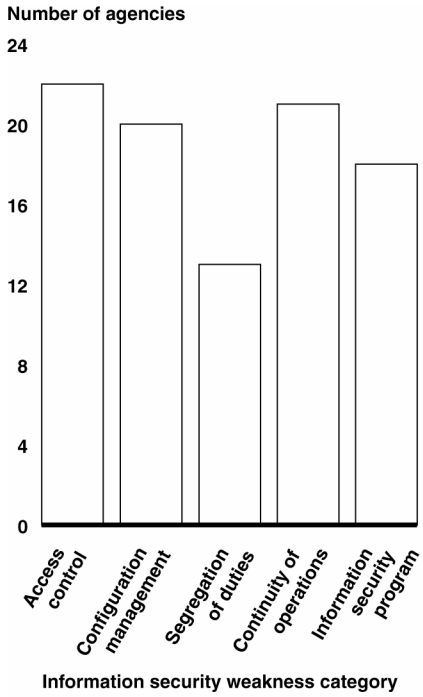
Figure 1: Agencies Reporting of Information Security Controls in Fiscal Year 2006 Financial Statement Audits



Source: GAO analysis.

Persistent weaknesses appear in 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. Figure 2 shows the number of major agencies that had weaknesses in these five areas.

Figure 2: Information Security Weaknesses at the 24 Major Agencies for Fiscal Year 2006



Source: GAO analysis.

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. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, can be both electronic and physical. Electronic access controls include the use of passwords, access privileges, encryption, and audit logs. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft.

Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate access controls in

place to ensure that only authorized individuals could access or manipulate data. Of the 24 major agencies, 22 had access control weaknesses. 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. For instance, many of the data losses that occurred at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Shortcomings Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include policies, procedures, and techniques addressing configuration management to ensure that software patches are installed in a timely manner; appropriately segregating incompatible duties; and establishing continuity of operations planning.

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. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

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 all the FISMA-required elements for an agencywide information security program. 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. Our analysis determined that at least 18 of the 24 major federal agencies had not fully 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 actions. For example,

- One agency had no documented process for conducting risk assessments, while another agency had outdated risk assessments. Another agency had assessed and categorized system risk levels and conducted risk assessments, but did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them.
- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance on how to guard against significant security weaknesses regarding topics such as physical access, Privacy Act-protected data, wireless configurations, and business impact analyses.
- Instances existed where security plans were incomplete or not up-to-date.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.
- Our report[8] on testing and evaluating security controls revealed that agencies had not adequately designed and effectively implemented

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

policies for testing their security controls in accordance with OMB and NIST guidance. 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.

- Our report on security controls testing also 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. We also found that some deficiencies had not been corrected in a timely manner.

  As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency, and responsibilities may be unclear, misunderstood, and improperly implemented. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. 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.

Examples Illustrate Weaknesses at Agencies

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.[9] 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 could gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its services.

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

- The Securities and Exchange Commission had made important progress addressing previously reported information security control weaknesses.[10] However, 15 new information security weaknesses pertaining to 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.
- The IRS had made limited progress toward correcting previously reported information security weaknesses at two data processing sites.[11] IRS had not consistently implemented effective access controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. These 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 air traffic control systems.[12] For example, 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. As a result, it was at increased risk of unauthorized system access, possibly

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

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

[12]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).

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 sophisticated hackers.

- Certain information security controls over a critical internal Federal Bureau of Investigation (FBI) network were ineffective in protecting the confidentiality, integrity, and availability of information and information resources.[13] 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. Taken 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.
- The Federal Reserve 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.[14] Specifically, the Federal Reserve 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

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

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

(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 maintained and operated on behalf of BPD were at an increased risk of unauthorized and possibly undetected use, modification, destruction, and disclosure. Furthermore, other applications that share common network resources with the distributed-based systems may face similar risks.

- Although the Centers for Medicare & 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.[15] 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 medical information transmitted on the network at increased risk of unauthorized disclosure and could result in a disruption in service.

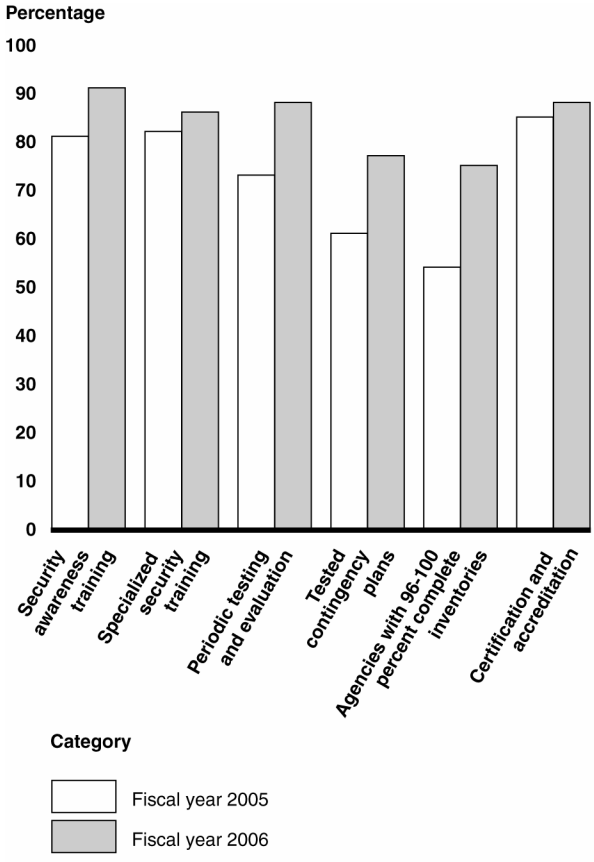
Improvements Reported in Performance Metrics, but Shortcomings Exist

Despite having persistent information security weaknesses, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006 reporting (see fig. 3), 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

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

accredited. However, IGs at several agencies sometimes disagreed with the information reported by the agency and have identified weaknesses in the processes used to implement these and other security program activities.

Figure 3: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of agency data.

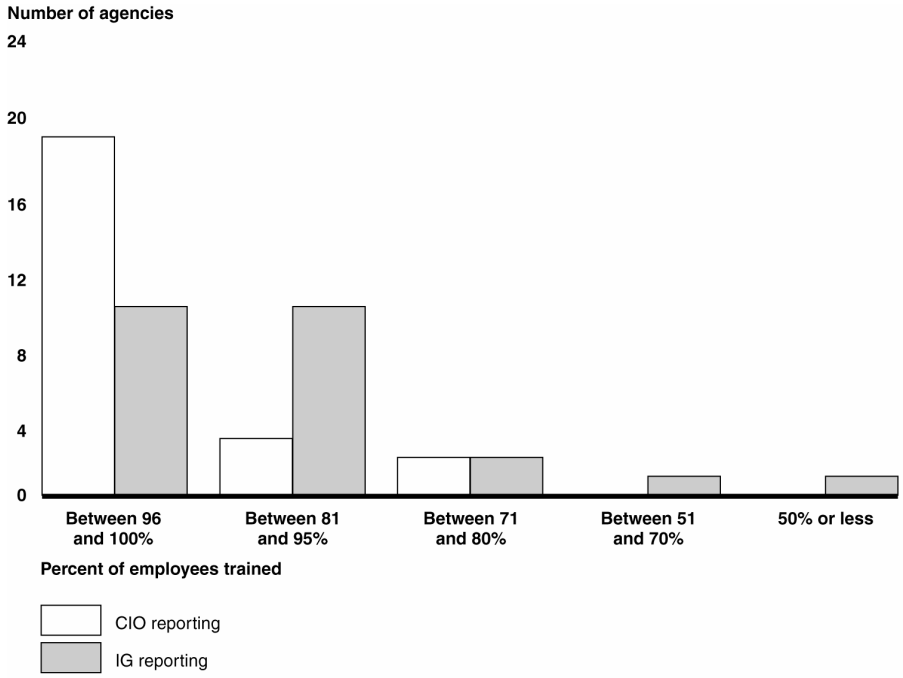
Information Security Training

The majority of agencies reported that more than 90 percent of their employees and contractors received IT security awareness training in fiscal year 2006. This is an increase from what we reported in 2006, where approximately 81 percent of employees governmentwide received IT security awareness 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.

Although agencies have reported improvements both in the number of employees receiving security awareness training and the number of employees who have significant security responsibilities and received 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 4 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 employees who are not fully aware of their security roles and responsibilities.

Figure 4: Percentage of Employees Receiving Security Awareness Training As Reported by Agencies and IGs



Source: GAO analysis.

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

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 evaluating of security controls. For example, IGs 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

The number of systems with tested contingency plans varied by the risk level of the system. Federal agencies reported that 77 percent of total systems had contingency plans that had been tested, up from 61 percent in 2005. However, on average, high-risk systems had the smallest percentage of tested contingency plans compared to other risk levels —only 64 percent of high-risk systems had tested contingency plans.

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, testing contingency plans, and certifying and accrediting systems. 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.

The total number of systems in some agencies' inventories varied widely from 2005 to 2006. In one case, an agency had a 300 percent increase in the number of systems, while another had approximately a 50 percent reduction in the number of their systems. IGs identified

some 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 efficiently 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

Federal agencies continue to report increasing percentages of systems completing 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 to 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.

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. For fiscal year 2006, ten IGs rated their agencies' certification and accreditation process as poor or failing—an increase from last year. 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 per NIST guidance or finding those items missing from certification and accreditation packages. 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. In other cases, systems were certified and accredited, but controls or contingency plans were not properly tested. 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.

Policies and Procedures

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. Another IG noted that three of the agency's components did not have overall configuration policies and that other components, which had 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

Shortcomings exist in agencies' security incident reporting procedures. According to the US-CERT[16] 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. However, 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,

[16]FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by DHS's US-CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

although it reported more than 800 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

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.

Opportunities Exist to Enhance Reporting and Independent Evaluations

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.

Limited Assurance of the Quality of Agency Processes

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. OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. However, 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. OMB has recognized the need for assurance of quality for agency processes. For example, it specifically requested that the IGs evaluate the certification and accreditation process. The qualitative assessments of the process allows the IG to rate its agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing." 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.

Reporting Does Not Include Aspects of Key Activities

Currently, OMB reporting guidance and performance measures do not include complete reporting on certain key FISMA-related activities. For example, 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,[17] maintaining up-to-date patches is key to complying with

[17]GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

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. As a result, OMB and the Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

Office of Inspector General Evaluations of Implementation Varied

Although the IGs conducted annual evaluations, they did not have a common approach. We received copies of all 24 IG FISMA template submissions and 20 IG FISMA reports.[18] For these efforts, 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).
- Multiple IGs indicated in the 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 that the agency's inventory was missing certain Web applications and concluded that the agency's inventory was only

[18]Two agencies—the Departments of Education and Justice—did not complete full reports for fiscal year 2006; the audit reports for two other agencies—the Departments of Commerce and Veterans Affairs—are still considered "draft."

0-50 percent complete, although it also noted that, due to time constraints, it was unable to determine whether other items were missing.

- Two IGs indicated basing a portion of their template submission solely on information provided to them by the agency, without conducting further investigation.
- 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. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency. A commonly used framework or methodology for the FISMA independent evaluations is a mechanism that could provide improved effectiveness, increased efficiency, and consistency of application. Such a framework may provide improved effectiveness of the annual evaluations by ensuring that compliance with FISMA and all related guidance, laws, and regulations are considered in the performance of the evaluation. IGs may be able to use the framework to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently. Without a consistent framework, work completed by IGs may not provide information that is comparable for oversight entities to assess the governmentwide information security posture.

In summary, as illustrated by recent incidents at federal agencies, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all major agencies exhibit weaknesses in one or more areas of information security controls. Despite these persistent weaknesses, agencies have continued to report steady progress in implementing certain information security requirements. However, IGs sometimes disagreed with the agency's

reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Mr. Chairman, this concludes my statement. I am happy to answer any questions at this time.

Contacts and Acknowledgments

If you have any questions regarding this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Jeffrey Knott (Assistant Director), Larry Crosland, Nancy Glover, Min Hyun, and Jayne Wilson.

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