United States Government Accountability Office

GAO

Report to Congressional Committees

July 2009

INFORMATION SECURITY

Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses

GAO

Accountability ★ Integrity ★ Reliability

GAO-09-546

July 2009

INFORMATION SECURITY

Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-546, 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 that can have serious consequences—such as intrusions by malicious users, compromised networks, and the theft of intellectual property and personally identifiable information—and has identified information security as a governmentwide high-risk issue since 1997.

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

In accordance with the FISMA requirement that the Comptroller General report periodically to Congress, GAO's objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agencies' implementation of FISMA requirements. To address these objectives, GAO analyzed agency, inspectors general, Office of Management and Budget (OMB), and GAO reports.

What GAO Recommends

GAO is recommending that the Director of OMB take several actions, including revising guidance. OMB generally agreed with GAO's overall assessment of information security at agencies, but did not concur with one aspect of GAO's assessment of OMB's review activities.

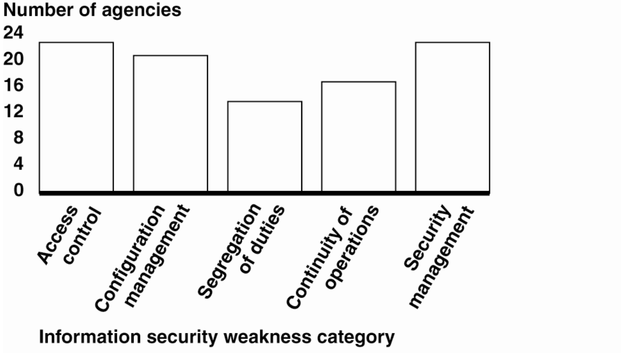
View GAO-09-546 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Persistent weaknesses in information security policies and practices continue to 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 of Americans, thereby exposing them to loss of privacy and identity theft. For fiscal year 2008, almost all 24 major federal agencies had weaknesses in information security controls (see figure). An underlying reason for these weaknesses is that agencies have not fully implemented their information security programs. As a result, agencies have limited assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise. In prior reports, GAO has made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls.

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. Agencies reported increased implementation of control activities, such as providing awareness training for employees and testing system contingency plans. However, agencies reported decreased levels of testing security controls and training for employees who have significant security responsibilities. In addition, inspectors general at several agencies disagreed with performance reported by their agencies and identified weaknesses in the processes used to implement these activities. Further, although OMB took steps to clarify its reporting instructions to agencies for preparing fiscal year 2008 reports, the instructions did not request inspectors general to report on agencies' effectiveness of key activities and did not always provide clear guidance to inspectors general. As a result, the reporting may not adequately reflect agencies' implementation of the required information security policies and procedures.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2008



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

Contents

Tables

Figures

Abbreviations

CD	compact disk
CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IG	Inspector General
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
US-CERT	U. S. Computer Emergency Readiness Team
US-VISIT	U. S. Visitor and Immigrant Status Indicator Technology

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 17, 2009

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 Edolphus Towns
Chairman
The Honorable Darrell Issa
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

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 increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology.

Over the past few years, 24 major federal agencies[1] have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to a loss of privacy, identity theft, and other

[1] The 24 major departments and agencies (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.

financial crimes. Since 1997, we have identified information security as a governmentwide high-risk issue in our biennial reports to Congress.[2]

Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[3] which requires agencies to develop and implement an information security program, evaluation processes, and annual reporting. FISMA requires mandated annual reports by federal agencies, the Office of Management and 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 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) federal agencies' implementation of FISMA requirements. To accomplish these objectives, we analyzed agency, inspector general, OMB, and our reports on information security. Where possible, we categorized findings from those reports into areas defined by FISMA and the Federal Information System Controls Audit Manual.[4] 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.

We conducted this performance audit from December 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For more details on our objectives, scope, and methodology, see appendix I.

[2] Most recently, GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

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

[4] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

Background

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risks to federal systems are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology.

Recognizing the importance of securing federal systems and data, Congress passed FISMA in 2002. The act sets 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; 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, inspectors general, and NIST. It also assigns responsibilities to OMB that 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.

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, FISMA requires information security programs to include, among other things:

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

- 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 actions 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 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 elements such 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.

As required by FISMA, NIST has prepared its annual public report on activities undertaken in the previous year and planned for the coming year. In addition, NIST's FISMA initiative supports the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies.

Responsibilities of Inspectors General

Under FISMA, the inspector general for each agency shall 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 inspector general, evaluations of non-national 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 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;
- 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.

Weaknesses in Information Security Place Sensitive Information at Risk

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. These persistent weaknesses expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. Further, our work and reviews by inspectors general note significant information security control deficiencies that place a broad array of federal operations and assets at risk. Consequently, we have made hundreds of recommendations to agencies to address these security control deficiencies.

Reported Incidents Are on the Rise and Place Sensitive Information at Risk

Since our report in July 2007, federal agencies have reported a spate of security incidents that have put sensitive data at risk, thereby exposing the personal information of millions of Americans to the 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 examples, reported in 2008 and 2009, illustrate that a broad array of federal information and assets remain at risk.

- In May 2009, the Department of Transportation Inspector General issued the results of an audit of Web applications security and intrusion detection in air traffic control systems at the Federal Aviation Administration (FAA). The inspector general reported that Web applications used in supporting air traffic control systems operations were not properly secured to prevent attacks or unauthorized access. To illustrate, vulnerabilities found in Web application computers associated with the Traffic Flow Management Infrastructure System, Juneau Aviation Weather System, and the Albuquerque Air Traffic Control Tower allowed audit staff to gain unauthorized access to data stored on these computers, including program source code and sensitive personally identifiable information. In addition, the inspector general reported that it found a vulnerability on FAA Web applications that could allow attackers to execute malicious codes on FAA users' computers, which was similar to an actual incident that occurred in August 2008. In February 2009, the FAA notified employees that an agency computer had been illegally accessed and employee personal identity information had been stolen electronically. Two of the 48 files on the breached computer server contained personal information about more than 45,000 FAA employees and retirees who were on the FAA payrolls as of the first week of February 2006. Law enforcement agencies were notified and are investigating the data theft.

- In March 2009, U.S. Congressman Jason Altmire and U.S. Senator Bob Casey announced that that they had sent a letter to the Under Secretary of Defense for Acquisition, Technology, and Logistics, asking for additional information on a recent security breach of the presidential helicopter, Marine One. According to the announcement, in February 2009, a company based in Cranberry, Pennsylvania, discovered that engineering and communications documents containing key details about the Marine One fleet had been downloaded to an Internet Protocol (IP) address in Iran. The documents were traced back to a defense contractor in Maryland, where an employee most likely downloaded a file-sharing program that inadvertently allowed others to access this information. According to information from the Congressman's Web site, recent reports have said that the federal government was warned last June that an Internet Web site with an IP address traced to Iran was actively seeking this information.

- In March 2009, the United States Computer Emergency Readiness Team (US-CERT) issued an updated notice to warn agencies and organizations of the Conficker/Downadup worm activity and to help prevent further compromises from occurring. In the notice, US-CERT warned that the Conficker/Downadup worm could infect a Microsoft Windows system from a thumb drive, a network share, or directly across a network if the host is not patched.

- According to a March 2009 media release from Senator Bill Nelson's office, cyber-invaders thought to be in China hacked into the computer network in Senator Nelson's office. There were two attacks on the same day in March 2009, and another one in February 2009 that targeted work stations used by three of Senator Nelson's staffers. The hackers were not able to take any classified information because that information is not kept on office computers, a spokesman said. The media release stated that similar incursions into computer networks in Congress were up significantly in the past few months.

- The Department of Energy's Office of Health, Safety, and Security announced that a password-protected compact disk (CD) had been lost during a routine shipment on January 28, 2009. The CD contained personally identifiable information for 59,617 individuals who currently work or formerly worked at facilities at the Department of Energy's Idaho site. The investigation verified that protection measures had been applied in accordance with requirements applicable to organizations working under cooperative agreements and surmised that while the CD had been lost for 8 weeks at the time of the investigation, no evidence had been found that revealed that the personal information on the lost disk had been compromised. The investigation concluded that OMB and Department of Energy requirements for managing and reporting the loss of the information had not been transmitted to the appropriate organizations and that there was a failure to provide timely notifications of the actual or suspected loss of information in this incident.

- In January 2009, the Program Director of the Office of Personnel and Management's USAJOBS Web site announced that their technology provider's (Monster.com) database had been illegally accessed and contact and account data had been taken, including user IDs and passwords, e-mail addresses, names, phone numbers, and some basic demographic data. The director pointed out that e-mail could be used for phishing activity and advised users to change their site login password.

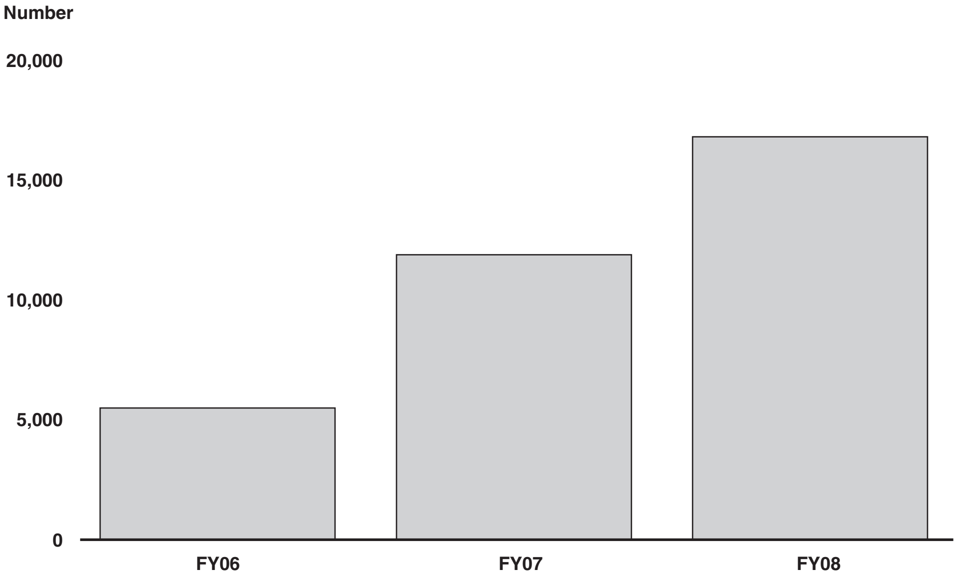
- In December 2008, the Federal Emergency Management Administration was alerted to an unauthorized breach of private information when an applicant notified it that his personal information pertaining to Hurricane Katrina had been posted on the Internet. The information posted to Web sites contained a spreadsheet with 16,857 lines of data that included applicant names, social security numbers, addresses, telephone numbers, e-mail addresses, and other information on disaster applicants who had evacuated to Texas. According to the Federal Emergency Management Administration, it took action to work with the Web site hosting the private information, and have that information removed from public view. Additionally, the agency reported that it worked to remove the same information from a second Web site. Further, the agency stated that while it believed most of the applicant information posted on the Web sites were properly released by them to a state agency, it did not authorize the subsequent public posting of much of this data.

- In June 2008, the Walter Reed Army Medical Center reported that officials were investigating the possible disclosure of personally identifiable information through unauthorized sharing of a data file containing the names of approximately 1,000 Military Health System beneficiaries. Walter Reed officials were notified of the possible exposure on May 21 by an outside company. Preliminary results of an ongoing investigation identified a computer from which the data had apparently been compromised. Data security personnel from Walter Reed and the Department of the Army think it is possible that individuals named in the file could become victims of identity theft. The compromised data file did not include protected health information such as medical records, diagnosis, or prognosis for patients.

- In March 2008, media reports surfaced noting that the passport files of three U.S. senators, who were also presidential candidates, had been improperly accessed by Department of State employees and contractor staff. As of April 2008, the system contained records on about 192 million passports for about 127 million passport holders. These records included personally identifiable information, such as the applicant's name, gender, social security number, date and place of birth, and passport number. In July 2008, after investigating this incident, the Department of State's Office of Inspector General reported many control weaknesses—including a general lack of policies, procedures, guidance, and training—relating to the prevention and detection of unauthorized access to passport and applicant information and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has risen dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (slightly more than 200 percent).

Figure 1: Incidents Reported to US-CERT, FY 2006-FY 2008



Source: GAO analysis of US-CERT data.

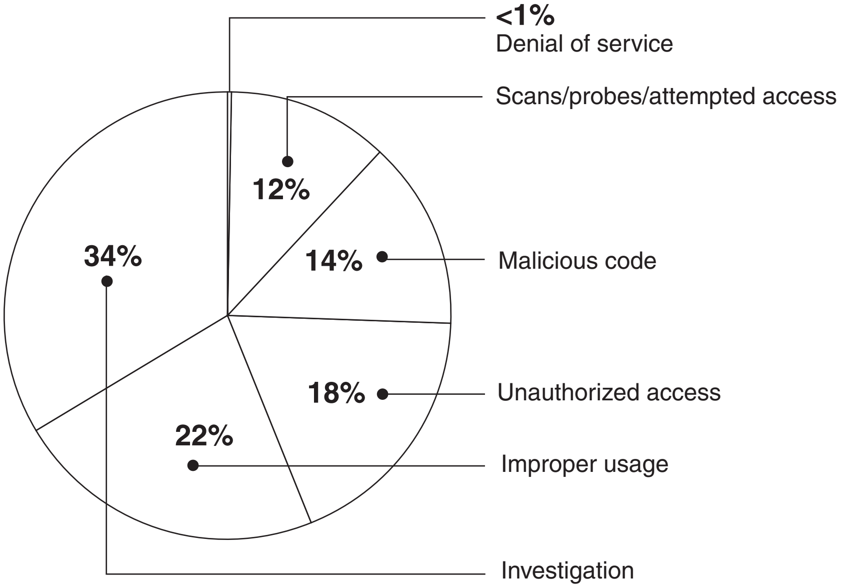
Agencies report the following types of incidents based on US-CERT-defined categories:

- **Unauthorized access:** Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.
- **Malicious code:** Installing 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:** Violating acceptable computing use policies.
- **Scans/probes/attempted access:** Accessing or identifying 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.

Under investigation: Investigating unconfirmed incidents that are potentially malicious, or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 2, the three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access, improper usage, and investigation (see fig. 2).

Figure 2: Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category



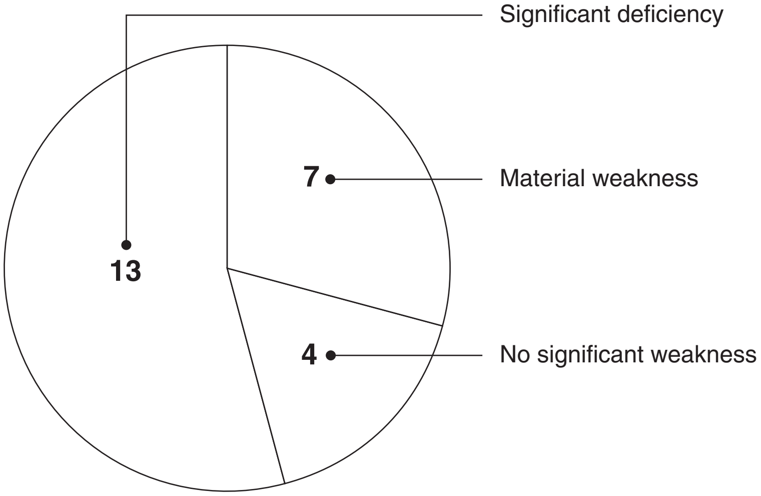
Source: GAO analysis of US-CERT data.

Weaknesses in Controls Highlight Deficiencies in the Implementation of Security Policies and Practices

Reviews at federal agencies continue to highlight deficiencies in their implementation of security policies and procedures. In their fiscal year 2008 performance and accountability reports, 20 of the 24 agencies indicated that inadequate information security controls were either a material weakness or a significant deficiency[6] (see fig. 3).

[6] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 3: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY 2008.

Similarly, in annual reports required under 31 U.S.C. § 3512 (commonly referred to as the *Federal Managers' Financial Integrity Act of 1982*),[7] 11 of 24 agencies identified material weaknesses in information security. Inspectors general have also noted weaknesses in information security, with 22 of 24 identifying it as a "major management challenge" for their agency.[8]

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example:

[7] FMFIA, Pub. L. No. 97-255, 96 Stat. 814 (Sept. 8, 1982), now codified at 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.

[8] The Reports Consolidation Act of 2000, Pub. L. No. 106-531, 114 Stat. 2537 (Nov. 22, 2000), requires inspectors general to include in their agencies' performance and accountability reports a statement that summarizes what they consider to be the most serious management and performance challenges facing their agencies and briefly assesses their agencies' progress in addressing those challenges. 31 U.S.C. § 3516(d).

- In 2009, we reported that security weaknesses at the Securities and Exchange Commission continued to jeopardize the confidentiality, integrity, and availability of the commission's financial and sensitive information and information systems.[9] Although the commission had made progress in correcting previously reported information security control weaknesses, it had not completed action to correct 16 weaknesses. In addition, we identified 23 new weaknesses in controls intended to restrict access to data and systems. Thus, the commission had not fully implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it had not always (1) consistently enforced strong controls for identifying and authenticating users, (2) sufficiently restricted user access to systems, (3) encrypted network services, (4) audited and monitored security-relevant events for its databases, and (5) physically protected its computer resources. The Securities and Exchange Commission also had not consistently ensured appropriate segregation of incompatible duties or adequately managed the configuration of its financial information systems. As a result, the Securities and Exchange Commission was at increased risk of unauthorized access to and disclosure, modification, or destruction of its financial information, as well as inadvertent or deliberate disruption of its financial systems, operations, and services. The Securities and Exchange Commission agreed with our recommendations and stated that it plans to address the identified weaknesses.

- In 2009, we reported that the Internal Revenue Service had made progress toward correcting prior information security weaknesses, but continued to have weaknesses that could jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information.[10] These deficiencies included some related to controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, as well as a control important in mitigating software vulnerability risks. For example, the agency continued to, among other things, allow sensitive information, including IDs and passwords for mission-critical applications, to be readily available to any user on its internal network and to grant excessive access to individuals who do not need it. In addition, the Internal Revenue Service had systems running unsupported software that could not be patched against known

[9] GAO, *Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls*, GAO-09-203 (Washington, D.C.: Mar. 16, 2009).

[10] GAO, *Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS*, GAO-09-136 (Washington, D.C.: Jan. 9, 2009).

vulnerabilities. Until those weaknesses are corrected, the Internal Revenue Service remains vulnerable to insider threats and is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services. The IRS agreed to develop a plan addressing each of our recommendations.

- In 2008, we reported that although the Los Alamos National Laboratory—one of the nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources.[11] As a result, sensitive information on the network—including unclassified controlled nuclear information, naval nuclear propulsion information, export control information, and personally identifiable information—were exposed to an unnecessary risk of compromise. Moreover, the risk was heightened because about 300 (or 44 percent) of 688 foreign nationals who had access to the unclassified network as of May 2008 were from countries classified as sensitive by the Department of Energy, such as China, India, and Russia. While the organization did not specifically comment on our recommendations, it agreed with the conclusions.

- In 2008, we reported that the Tennessee Valley Authority had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities we reviewed.[12] Multiple weaknesses within the Tennessee Valley Authority corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example, almost all of the workstations and servers that we examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore,

[11] GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

[12] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008) and *Information Security: TVA Needs to Enhance Security of Critical Infrastructure Controls Systems and Networks*, GAO-08-755T (Washington, D.C.: May 21, 2008).

Tennessee Valley Authority had not adequately secured its control system networks and devices on these networks, leaving the control systems vulnerable to disruption by unauthorized individuals. In addition, we reported that the network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. Specifically, weaknesses in the separation of network segments could allow an individual who had gained access to a computing device connected to a less secure portion of the network to be able to compromise systems in a more secure portion of the network, such as the control systems. As a result, Tennessee Valley Authority's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats and could affect its ability to properly generate and deliver electricity. The Tennessee Valley Authority agreed with our recommendations and provided information on steps it was taking to implement them.

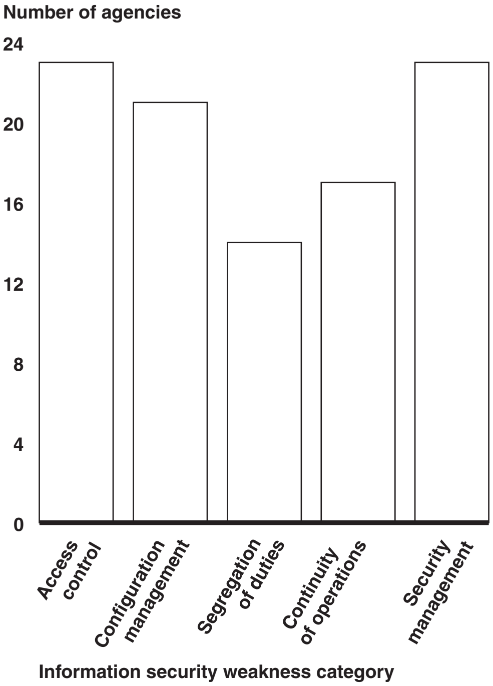
- In 2007, we reported that the Department of Homeland Security had significant weaknesses in computer security controls surrounding the information systems used to support its U.S. Visitor and Immigrant Status Technology (US-VISIT) program for border security.[13] For example, it had not implemented controls to effectively prevent, limit, and detect access to computer networks, systems, and information. Specifically, it had not (1) adequately identified and authenticated users in systems supporting US-VISIT; (2) sufficiently limited access to US-VISIT information and information systems; (3) ensured that controls adequately protected external and internal network boundaries; (4) effectively implemented physical security at several locations; (5) consistently encrypted sensitive data traversing the communication network; and (6) provided adequate logging or user accountability for the mainframe, workstations, or servers. In addition, it had not always ensured that responsibilities for systems development and system production had been sufficiently segregated and had not consistently maintained secure configurations on the application servers and workstations at a key data center and ports of entry. As a result, increased risk existed that unauthorized individuals could read, copy, delete, add, and modify sensitive information—including personally identifiable information—and disrupt service on Customs and Border Protection systems supporting the US-VISIT program. The department stated that it directed Customs and Border Protection to complete remediation activities to address each of our recommendations.

[13] GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, GAO-07-870 (Washington, D.C.: July 13, 2007).

Weaknesses Persist in All Major Categories of Controls

According to our reports and those of agency inspectors general, persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs 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 4.

Figure 4: Information Security Weaknesses at 24 Major Agencies for FY 2008



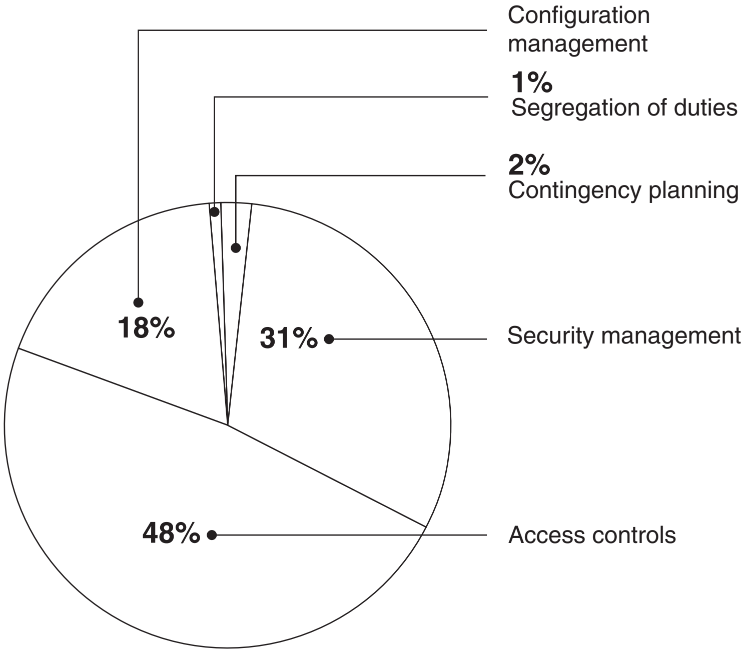
Source: GAO analysis of IG, agency, and GAO reports.

Access Controls Were Not Adequate

Agencies use access controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized use, modification, disclosure, and loss. Such controls include both electronic and physical controls. Electronic access controls include those related to boundary protection, user identification and authentication, authorization, cryptography, and auditing and monitoring. Physical access 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.

At least 23 major federal agencies had access control weaknesses during fiscal year 2008. An analysis of our reports reveals that 48 percent of information security control weaknesses pertained to access controls (see fig. 5). For example, agencies did not consistently (1) establish sufficient boundary protection mechanisms; (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 encryption to protect sensitive data on networks and portable devices; (5) log, audit, and monitor security-relevant events; and (6) establish effective controls to restrict physical access to information assets. Without adequate access controls in place, agencies cannot ensure that their information resources are protected from intentional or unintentional harm.

Figure 5: Control Weaknesses Identified in GAO Reports, May 2007-April 2009



Source: GAO analysis of prior GAO reports.

Boundary Protection

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. Agencies segregate the parts of their networks that are publicly accessible by placing these components in subnetworks with separate physical interfaces and preventing public access to their internal networks. Unnecessary connectivity to an agency'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. In addition to deploying a series of security technologies at multiple layers, deploying diverse technologies at different layers helps to mitigate the risk of successful cyber attacks. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection technologies can be deployed to defend against attacks from the Internet.

Agencies continue to demonstrate vulnerabilities in establishing appropriate boundary protections. For example, two agencies that we assessed did not adequately secure channels to connect remote users, increasing the risk that attackers will use these channels to gain access to restricted network resources. One of these agencies also did not have adequate intrusion detection capabilities, while the other allowed users of one network to connect to another, higher-security network. Such weaknesses in boundary protections impair an agency's ability to deflect and detect attacks quickly and protect sensitive information and networks.

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.

Agencies did not always adequately control user accounts and passwords to ensure that only valid users could access systems and information. In our 2007 FISMA report,[14] we noted several weaknesses in agencies' identification and authentication procedures. Agencies continue to experience similar weaknesses in fiscal years 2008 and 2009. For example, certain agencies did not adequately enforce strong password settings, increasing the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information. In other instances, agencies did not enforce periodic changing of passwords or use of one-time passwords or passcodes, and transmitted or stored passwords in clear text. Poor password management increases the risk that unauthorized users could guess or read valid passwords to devices and use the compromised devices for an indefinite period of time.

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, which is a basic principle for

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

securing computer resources and information and 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, agencies 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 agency must give careful consideration to its assignment of rights and permissions.

Agencies continued to grant rights and permissions that allowed more access than users needed to perform their jobs. Inspectors general at 12 agencies reported instances where users had been granted excessive privileges. In our reviews, we also noted vulnerabilities in this area. For example, at one agency, users could inappropriately escalate their access privileges to run commands on a powerful system account, many had unnecessary and inappropriate access to databases, and other accounts allowed excessive privileges and permissions. Another agency allowed (on financial applications) generic, shared accounts that included the ability to create, delete, and modify users' accounts. Approximately 1,100 users at yet another agency had access to mainframe system management utilities, although such access was not necessarily required to perform their jobs. These utilities provided access to all files stored on disk; all programs running on the system, including the outputs; and the ability to alter hardware configurations supporting the production environment. We uncovered one agency that had provided a contractor with system access that was beyond what was needed, making the agency vulnerable to incidents on the contractor's network. Another agency gave all users of an application full access to the application's source code although their responsibilities did not require this level of privilege. Such weaknesses in authorization place agencies at increased risk of inappropriate access to data and sensitive system programs, as well as to the consequent disruption of services.

Cryptography

Cryptography[15] 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 recommends disabling protocols that do not encrypt information transmitted across the network, such as user identification and password combinations.

Agencies did not always encrypt sensitive information on their systems or traversing the network. In our reviews of agencies' information security, we found that agencies did not always encrypt sensitive information. For example, five agencies that we reviewed did not effectively use cryptographic controls to protect sensitive resources. Specifically, one agency allowed unencrypted protocols to be used on its network devices. Another agency did not require encrypted passwords for network logins, while another did not consistently provide approved, secure transmission of data over its network. 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.

Auditing 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. Agencies 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 agencies configure system or security software determines the nature and extent of the information that can be provided by the audit trail. To be effective, agencies should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events.

[15] 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 on their network. For example, agencies did not monitor critical portions of their networks for intrusions; record successful, unauthorized access attempts; log certain changes to data on a mainframe (which increases the risk of compromised security controls or disrupted operations); and capture all authentication methods and logins to a network by foreign nationals. Similarly, 14 agencies did not always have adequate auditing and monitoring capabilities. For example, one agency did not conduct a baseline assessment of an important network. This baseline determines a typical state or pattern of network activity. Without this information, the agency could have difficulty detecting and investigating anomalous activity to ascertain whether or not an attack was under way. Another agency did not perform source code scanning or have a process for manual source code reviews, which increases the risk that vulnerabilities would not be detected. As a result, unauthorized access could go undetected, and if a system is modified or disrupted, the ability to trace or recreate events could be impeded.

Physical Security

Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to sensitive computing and communications resources, usually by limiting access to the buildings and rooms in which the resources are housed. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources. Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security also include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas must be managed appropriately.

Our analysis of inspector general, GAO, and agency reports has shown that nine agencies did not sufficiently restrict physical access to sensitive computing and communication resources. The physical security measures employed by these agencies often did not comply with their own requirements or with federal standards. Access to facilities containing sensitive equipment and information was not always adequately restricted. For example, at one agency with buildings housing classified networks, cars were not stopped and inspected; a sign indicated the building's purpose; fencing was scalable; and access to buildings containing computer network equipment was not controlled by electronic or other means. Agencies did not adequately manage visitors, in one instance, placing network jacks in an area where unescorted individuals could use them to obtain electronic access to restricted computing resources, and in another failing to properly identify and control visitors at a facility containing sensitive equipment. Agencies did not always remove employees' physical access authorizations to sensitive areas in a timely manner when they departed or their work no longer required such access. Environmental controls at one agency did not meet federal guidelines, with fire suppression capabilities, emergency lighting, and backup power all needing improvements. Such weaknesses in physical access controls increase the risk that sensitive computing resources will inadvertently or deliberately be misused, damaged, or destroyed.

Configuration Management Controls Were Not Always 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.

Twenty-one agencies demonstrated weaknesses in configuration management controls. For instance, several agencies did not implement common secure configuration policies across their systems, increasing the risk of avoidable security vulnerabilities. In addition, agencies did not effectively ensure that system software changes had been properly authorized, documented, and tested, which increases the risk that unapproved changes could occur without detection and that such changes could disrupt a system's operations or compromise its integrity. Agencies did not always monitor system configurations to prevent extraneous services and other vulnerabilities from remaining undetected and jeopardizing operations. At least six agencies did not consistently update software on a timely basis to protect against known vulnerabilities or did not fully test patches before applying them. Without a consistent approach to updating, patching, and testing software, agencies are at increased risk of exposing critical and sensitive data to unauthorized and possibly undetected access.

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 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 14 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, an individual who enters an applicant's data into a financial system also had the ability to hire the applicant. At another agency, 76 system users had the ability to create and approve purchase orders. Without adequate segregation of duties, there is an increased risk that erroneous or fraudulent actions can occur, improper program changes can be implemented, and computer resources can be damaged or destroyed.

Continuity of Operations Plans Have Shortcomings

An agency 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 a catastrophe 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 to ensure that critical information systems, operations, and data such as financial processing and related records can be properly restored if an emergency or a disaster occurs. To ensure that the plan is complete and fully understood by all key staff, it should be tested— including unannounced tests—and test plans and results documented to provide a basis for improvement. If continuity of operations controls are inadequate, even relatively minor interruptions could result in lost or incorrectly processed data, which could cause financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.

Although agencies have reported increases in the number of systems for which contingency plans have been tested, at least 17 agencies had shortcomings in their continuity of operations plans. For example, one agency's disaster recovery planning had not been completed. Specifically, disaster recovery plans for three components of the agency were in draft form and had not been tested. Another agency did not include a business impact analysis in the contingency plan control, which would assist in planning for system recovery. In another example, supporting documentation for some of the functional tests at the agency did not adequately support testing results for verifying readability of backup tapes retrieved during the tests. Until agencies complete actions to address these weaknesses, they are at risk of not being able to appropriately recover systems 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, as 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.

Twenty-three agencies had not fully or effectively implemented agencywide information security programs. Agencies often did not adequately design or effectively implement policies for elements key to an information security program. Weaknesses in agency information security program activities, such as risk assessments, information security policies and procedures, security planning, security training, system testing and evaluation, and remedial action plans are described next.

Risk Assessments

In order for agencies to determine what security controls are needed to protect their information resources, they must first identify and assess their information security risks. Moreover, by increasing awareness of risks, these assessments can generate support for policies and controls.

Agencies have not fully implemented their risk assessment processes. In addition, 14 major agencies had weaknesses in their risk assessments. Furthermore, they did not always properly assess the impact level of their systems or evaluate potential risks for the systems we reviewed. For example, one agency had not yet finalized and approved its guidance for completing risk assessments. In another example, the agency had not properly categorized the risk to its system, because it had performed a risk assessment without an inventory of interconnections to other systems. Similarly, another agency had not completed risk assessments for its critical systems and had not assigned impact levels. In another instance, an agency had current risk assessments that documented residual risk assessed and potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities they had identified. However, that agency had not identified many of the vulnerabilities we found and had not subsequently assessed the risks associated with them. As a result of these weaknesses, agencies may be implementing inadequate or inappropriate security controls that do not address the systems' true risk, and potential risks to these systems may not be known.

Policies and Procedures

According to FISMA, each federal agency's information security program must include policies and procedures that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each agency's information system. The term 'security policy' refers to specific security rules set up by the senior management of an agency to create a computer security program, establish its goals, and assign responsibilities. Because policy is written at a broad level, agencies also develop standards, guidelines, and procedures that offer managers, users, and others a clear approach to implementing policy and meeting organizational goals.

Thirteen agencies had weaknesses in their information security policies and procedures. For example, one agency did not have updated policies and procedures for configuring operating systems to ensure they provide the necessary detail for controlling and logging changes. Another agency had not established adequate policies or procedures to implement and maintain an effective departmentwide information security program or to address key OMB privacy requirements. Agencies also exhibited weaknesses in policies concerning security requirements for laptops, user access privileges, security incidents, certification and accreditation, and physical security. As a result, agencies have reduced assurance that their systems and the information they contain are sufficiently protected. Without policies and procedures that are based on risk assessments, agencies may not be able to cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each agency's information system.

Security Plans

FISMA requires each federal agency to develop plans for providing adequate information security for networks, facilities, and systems or groups of systems. According to NIST 800-18, system security planning is an important activity that supports the system development life cycle and should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. The system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. NIST guidance also indicates that all security plans should be reviewed and updated, if appropriate, at least annually. Further, appendix III of OMB Circular A-130 requires security plans to include controls for, among other things, contingency planning and system interconnections.

System security plans were incomplete or out of date at several agencies. For example, one agency had an incomplete security plan for a key application. Another agency had only developed a system security plan that covered two of the six facilities we reviewed, and the plan was incomplete and not up-to-date. At another agency, 52 of the 57 interconnection security agreements listed in the security plan were not current since they had not been updated within 3 years. Without adequate security plans in place, agencies cannot be sure that they have the appropriate controls in place to protect key systems and critical information.

Specialized Training

Users of information resources can be one of the weakest links in an agency's ability to secure its systems and networks. Therefore, an important component of an agency's information security program is providing the required training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks.

Several agencies had not ensured that all information security employees and contractors, including those who have significant information security responsibilities, had received sufficient training. For example, users of one agency's IT systems had not been trained to check for continued functioning of their encryption software after installation. At another agency, officials stated that several of its components had difficulty in identifying and tracking all employees who have significant IT security responsibilities and thus were unable to ensure that they received the specialized training necessary to effectively perform their responsibilities. Without adequate training, users may not understand system security risks and their own role in implementing related policies and controls to mitigate those risks.

System Tests and Evaluations

Another key element of an information security program is testing and evaluating system controls to ensure that they are appropriate, effective, and comply with policies. FISMA requires that agencies test and evaluate the information security controls of their major systems and that the frequency of such tests be based on risk, but occur no less than annually. NIST requires agencies to ensure that the appropriate officials are assigned roles and responsibilities for testing and evaluating controls over their systems.

Agencies did not always implement policies and procedures for performing periodic testing and evaluation of their information security controls. For example, one agency had not adequately tested security controls. Specifically, the tests of a major application and the mainframe did not identify or discuss the vulnerabilities that we had identified during our audit. The same agency's testing did not reveal problems with the mainframe that could allow unauthorized users to read, copy, change, delete, and modify data. In addition, although testing requirements were stated in test documentation, the breadth and depth of the test, as well as the results of the test, had not always been documented. Also, agencies reported inconsistent testing of security controls among components. Without conducting the appropriate tests and evaluations, agencies have limited assurance that policies and controls are appropriate and working as intended. Additionally, there is an increased risk that undetected vulnerabilities could be exploited to allow unauthorized access to sensitive information.

Remedial Action Processes and Plans

FISMA requires that agencies' information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency.

Since our 2007 FISMA report, we have continued to find weaknesses in agencies' plans and processes for remedial actions. Agencies indicated that they had corrected or mitigated weaknesses; however, our work revealed that those weaknesses still existed. In addition, the inspectors general at 14 of the 24 agencies reported weaknesses in the plans to document remedial actions. For example, at several agencies, the inspector general reported that weaknesses had been identified but not documented in the remediation plans. Inspectors general further reported that agency plans did not include all relevant information in accordance with OMB instructions. We also found that deficiencies had not been corrected in a timely manner. Without a mature process and effective remediation plans, the 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, their systems and information will remain at increased risk of attack or compromise.

Opportunities Exist for Bolstering Federal Information Security

In prior reports,[16] we and inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and continuity of operations planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

[16] See related GAO products for a list of our recent reports on information security.

In March 2009, we reported on 12 key improvements suggested by a panel of experts as being essential to improving our national cyber security posture (see app. III).[17] The expert panel included former federal officials, academics, and private-sector executives. Their suggested improvements are intended to address many of the information security vulnerabilities facing both private and public organizations, including federal agencies. Among these improvements are recommendations to develop a national strategy that clearly articulates strategic objectives, goals, and priorities and to establish a governance structure for strategy implementation.

Due to increasing cyber security threats, the federal government has initiated several efforts to protect federal information and information systems. Recognizing the need for common solutions to improving security, the White House, OMB, and federal agencies have launched or continued several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed here.

- *60-day cyber review:* The National Security Council and Homeland Security Council recently completed a 60-day interagency review intended to develop a strategic framework to ensure that federal cyber security initiatives are appropriately integrated, resourced, and coordinated with Congress and the private sector. The resulting report recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, creating a new national cybersecurity strategy, and developing a framework for cyber research and development.[18]

- *Comprehensive National Cybersecurity Initiative:* In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[19] While these initiatives have not been made public, the Director of National Intelligence stated that they include defensive, offensive,

[17] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

[18] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[19] The White House, *National Security Presidential Directive 54/ Homeland Security Presidential Directive 23* (Washington, D.C.: Jan. 8, 2008).

research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[20]

- *The Information Systems Security Line of Business:* The goal of this initiative, led by OMB, is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.

- *Federal Desktop Core Configuration:* For this initiative, OMB directed agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by the National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security. The goal of this initiative is to improve information security and reduce overall IT operating costs.

- *SmartBUY:* This program, led by the General Services Administration, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections Initiative:* This effort, directed by OMB and led by the Department of Homeland Security, is designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of 50.

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

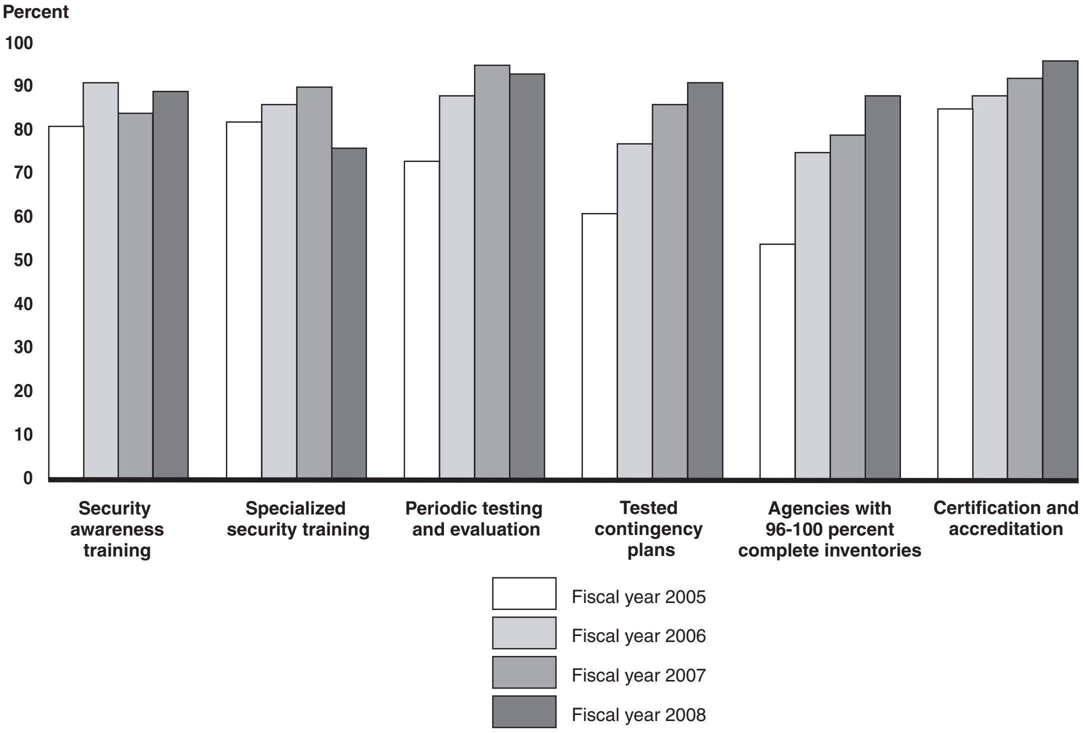
[20] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

Agencies Continue to Report Progress in Implementing Requirements

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. OMB also reported that agencies' were increasingly performing key activities. Specifically, agencies reported increases in the number and percentage of systems that had been certified and accredited,[21] the number and percentage of employees and contractors receiving security awareness training, and the number and percentage of systems with tested contingency plans. However, the number and percentage of systems that had been tested and evaluated at least annually decreased slightly and the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly (see fig. 6). Consistent with previous years, inspectors general continued to identify weaknesses with the processes and practices agencies have in place to implement FISMA requirements. Although OMB took steps to clarify its reporting instructions to agencies for preparing fiscal year 2008 reports, the instructions did not request inspectors general to report on agencies' effectiveness of key activities and did not always provide clear guidance to inspectors general.

[21] Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

Figure 6: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of IG and agency data.

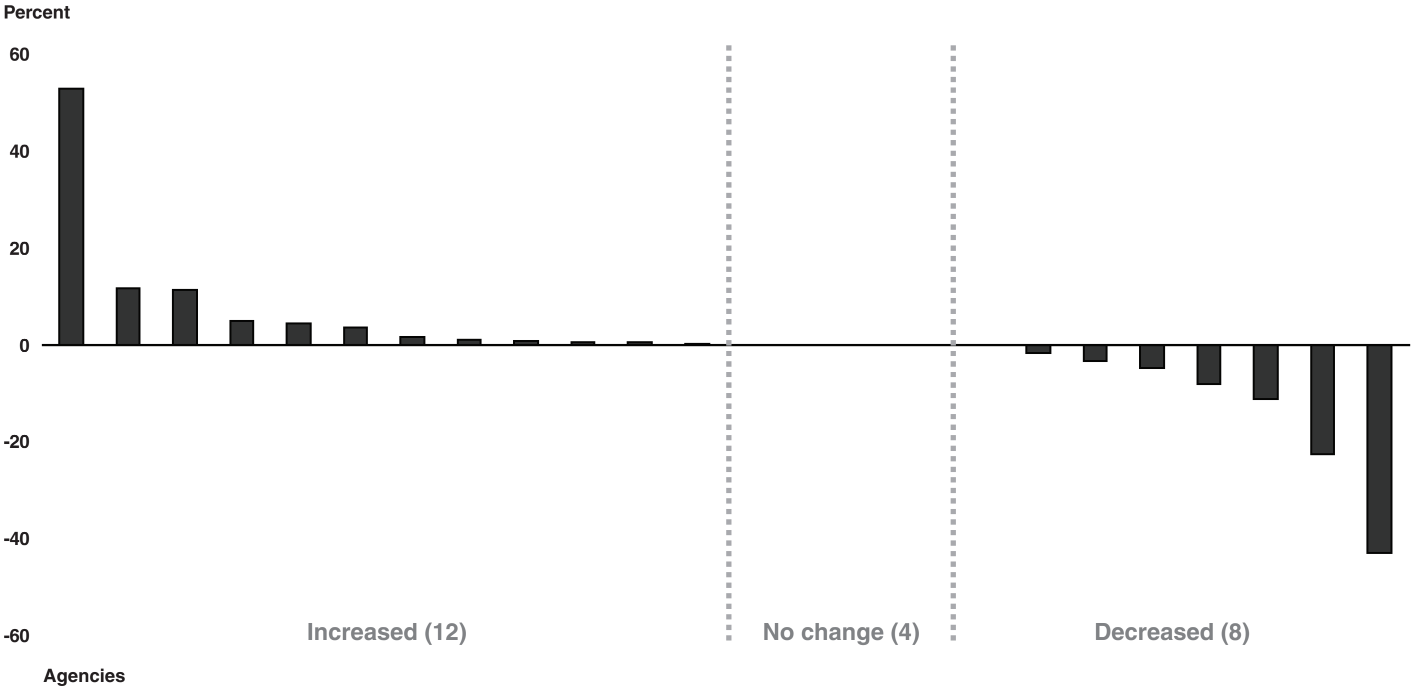
Agencies Report Mixed Progress in Implementing Security Awareness and Specialized Training

Federal agencies rely on their employees to protect the confidentiality, integrity, and availability of the information in their systems. It is critical for system users to understand their security roles and responsibilities and to be adequately trained to perform them. FISMA requires agencies to provide security awareness training to personnel, including contractors and other users of information systems that support agency operations and assets. This training should explain 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.

Agencies reported a slight increase in the percentage of employees and contractors who received security awareness training. According to agency reports, 89 percent of total employees and contractors had received security awareness training in 2008 compared to 84 percent of employees and contractors in 2007. While this change marks an improvement between fiscal years 2007 and 2008, the percentage of employees and contractors receiving security awareness training is still below the 91 percent reported for 2006. In addition, seven inspectors general reported disagreement with the percentage of employees and contractors receiving security awareness training reported by their agencies. Additionally, several inspectors general reported specific weaknesses related to security awareness training at their agencies; for example, one inspector general reported that the agency lacked the ability to document and track which system users had received awareness training, while another inspector general reported that training did not cover the recommended topics.

Governmentwide, agencies reported a lower percentage of employees who had significant security responsibilities who had received specialized training. In fiscal year 2008, 76 percent of these employees had received specialized training compared with 90 percent of these employees in fiscal year 2007. Although the governmentwide percentage decreased, the majority of the 24 agencies reported increasing or unchanging percentages of employees receiving specialized training; 8 of the 24 agencies reported percentage decreases (see fig. 7).

Figure 7: Specialized Training for 24 Major Agencies



Source: GAO analysis of agency data.

At least 12 inspectors general reported weaknesses related to specialized security training. One of the inspectors general reported that some groups did not have a training program for personnel who have critical IT responsibilities and another inspector general reported that the agency was unable to effectively track contractors who needed specialized training. Decreases in the number of individuals receiving specialized training at some federal agencies combined with continuing deficiencies in training programs could limit the ability of agencies to implement security measures effectively. Providing for the confidentiality, integrity, and availability of information in today's highly networked environment is not an easy or trivial task. The task is made that much more difficult if each person who owns, uses, relies on, or manages information and information systems does not know or is not properly trained to carry out his or her specific responsibilities.

Weaknesses Reported in Testing and Evaluating System Security Controls

Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an agency 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 inspector general 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, and operational and technical controls for every system identified in the agency's required inventory of major information systems. For the annual FISMA reports, OMB requires that agencies identify the number of agency and contractor systems for which security controls have been tested.

In 2008, federal agencies reported testing and reviewing security controls for 93 percent of their systems, a slight decline from 95 percent in 2007. Despite this percentage remaining above 90 percent, inspectors general continued to identify deficiencies in agencies' testing and evaluation of security controls for their systems. For example, one agency's inspector general reported that systems owners only reviewed documents to assess security controls and did not use other assessment methods as suggested by NIST guidance, such as selecting samples for testing and interviewing responsible parties. Another inspector general identified instances where the agency did not document the test results in the system's security test and evaluation report. In addition, two inspectors general reported that their agencies had not always tested the controls for their systems at least annually. As a result, agencies may not have reasonable assurance that controls have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency.

Agencies Reported Testing More Contingency Plans, but Inspectors General often Cited Weaknesses

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 tested in accordance with policy and guidance and requests that inspectors general also report this percentage for the subset of systems the inspector general selected for review.

Federal agencies reported that 91 percent of their systems had contingency plans that had been tested, an increase from 86 percent tested in fiscal year 2007. In addition, agencies reported progress in the number of high-risk systems with tested contingency plans; 90 percent of these systems had tested contingency plans, an increase from 77 percent in fiscal year 2007. Agencies also reported 92 percent of moderate-risk systems, 90 percent of low-risk systems, and 96 percent of uncategorized systems with tested contingency plans.

While agencies reported higher percentages of tested contingency plans, 14 inspectors general reported weaknesses in their agencies' contingency planning development and testing. For example, the inspector general of one agency reported that contingency plans were missing required elements. Regarding the testing of contingency plans, another inspector general reported that the agency had not ensured that the contractor had tested contingency plans or periodically conducted quality testing. At another agency, the inspector general reported that the agency had not performed a full, comprehensive disaster recovery test to ensure that essential and critical systems and applications could be recovered. Without developing contingency plans and ensuring that they are tested, an agency increases its risk that it will not be able to effectively recover and continue operations when an emergency occurs.

Agencies Reported More Systems, but Deficiencies Were Identified in Inventory Processes

In fiscal year 2008, 24 major agencies reported a total of 10,587 systems, composed of 8,685 agency and 1,902 contractor systems as shown by impact level in table 1. This represents a slight increase in the total number of systems from fiscal year 2007. Specifically, the number of agency systems decreased slightly and the number of contractor systems increased by 40 percent.

Table 1: Total Number of Agency and Contractor Systems in FY 2007 and FY 2008 by Impact Level

	Agency		Contractor		Total	
Impact level	**FY07**	**FY08**	**FY07**	**FY08**	**FY07**	**FY08**
High	1,089	1,043	121	113	**1,210**	**1,156**
Moderate	3,264	3,556	513	535	**3,777**	**4,091**
Low	4,351	3,943	334	738	**4,685**	**4,681**
Not categorized	229	143	384	516	**613**	**659**
Total	**8,933**	**8,685**	**1,352**	**1,902**	**10,285**	**10,587**

Source: GAO analysis of agency FY 2007 and FY 2008 FISMA reports.

Eleven inspectors general identified weaknesses in their agencies' inventory process. For example, one inspector general agreed that its agency's inventory accurately captured the number of active systems, but indicated the inventory had also included systems in development, which were not labeled as such and therefore could not be labeled and inventoried accurately. Another inspector general reported that its agency had not verified the inventory information reported by its components, but had instead relied on an honor system of reporting. Other weaknesses included contractor systems not listed in the inventory or an agency not having interfaces to other systems identified in its inventory. Without complete, accurate inventories, agencies cannot efficiently maintain and secure their systems.

Agencies Reported Higher Percentages, but Inspectors General Highlight Weaknesses in the Quality of Certifications and Accreditations

OMB has continued to emphasize its long-standing policy of requiring a management official to formally authorize (accredit) an information system to process information and accept the risk associated with its operation based on a formal evaluation (certification) of the system's security controls. For the annual FISMA reports, OMB requires agencies to identify the number of systems and impact levels authorized for processing after completing certification and accreditation. OMB requests that inspectors general also report this percentage for the subset of systems reviewed. In addition, OMB asks the inspectors general to rate the quality of the agency's certification and accreditation process on a scale of failing to excellent. Inspectors general may also indicate which aspects of the certification and accreditation process have been considered in determining that rating, such as the security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, configurations/patching, and other items. OMB's annual reporting template also allows the inspectors general to comment on their agencies' certification and accreditation processes.

Federal agencies reported higher percentages of systems that have been certified and accredited than in 2007. For fiscal year 2008, 96 percent of the agencies' systems were reported as being certified and accredited, as compared with 92 percent in 2007. In addition, agencies reported certifying and accrediting 98 percent of their high-risk systems, an increase from 95 percent in 2007.

Although agencies continue to report higher percentages of certified and accredited systems, inspectors general continue to report mixed results in the quality of the certification and accreditation processes at their agencies. To illustrate, 17 inspectors general reported specific weaknesses in their agency's certification and accreditation processes. For example, two inspectors general rated their agencies' certification and accreditation process as poor or failing, while both of those agencies reported that more than 90 percent of their systems had been certified and accredited. In another example, the inspector general of one agency stated that systems had been authorized to operate without sufficient testing of the adequacy of mandatory security controls. Inspectors general also cited other weaknesses, such as the security plan not providing an adequate basis for certification and accreditation and the risk assessment not identifying risks for vulnerabilities exposed by previous testing. Without ensuring the complete certification and accreditation of a system, agency officials may not have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

Agencies Report Having Configuration Management Policies, but Did Not Always Implement Them

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 an information security program; a key aspect of these policies and procedures is having minimally acceptable configuration standards. Configuration standards can 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 many of the 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 2008, for the first time, OMB required agencies to report on whether they had implemented security configurations prescribed under OMB's memorandum for Windows Vista and XP operating systems.[22] For annual FISMA reporting, OMB requires agencies to report whether they have an agencywide security configuration policy; the extent to which they have implemented common security configurations, including those available from the NIST Web site, on applicable systems; and whether or not they have adopted and implemented Windows XP and Vista standard configurations, documented deviations, and implemented the settings. OMB also requested inspectors general to report on their agencies' implementation of these configurations.

Reporting by agencies and inspectors general illustrates that, while many agencies had configuration policies, those policies had not always been implemented. All 24 major federal agencies reported that they had an agencywide security configuration policy. Even though 22 inspectors general agreed that their agency had such a policy, they did not agree that the implementation was always as high as the agencies had reported. For example, 12 agencies reported implementing common security configurations 96 to 100 percent of the time, but only 6 inspectors general reported this. In another example, only one agency reported implementing common security configurations 0 to 50 percent of the time, while seven inspectors general reported this level of implementation for their agencies. In addition, only seven agencies and six inspectors general reported that the agency had implemented standard security settings. If minimally acceptable configuration requirements policies are not properly implemented and applied to systems, agencies will not have assurance that products have been configured adequately to protect those systems, which could make them more vulnerable.

Most Agencies Reported Following Security Incident Procedures, but Weaknesses in Procedures Continue at Selected Agencies

Although strong controls may not block all intrusions and misuse, agencies 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 agency to improve its understanding of threats and the potential costs of security incidents, and doing so can pinpoint vulnerabilities that need to be addressed so that they are not exploited again.

[22] OMB, Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration* (Washington, D.C.: August 2008).

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 state whether or not the agency follows documented policies and procedures for reporting incidents internally, to the US-Computer Emergency Readiness Team (US-CERT), and to law enforcement. OMB also requires agencies to indicate additional information about their incident detection and monitoring capabilities, including what tools and technologies the agency uses for incident detection. For FISMA reporting, inspectors general are also requested to state whether or not their agencies follow documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement.

All of the agencies reported that they had followed policies and procedures for reporting incidents internally and to law enforcement during fiscal year 2008, and only one agency reported that it had not followed documented policies and procedures for reporting incidents to US-CERT.

While the majority of inspectors general continue to report that their agencies are following documented procedures for identifying and reporting incidents internally as well as to US-CERT and to law enforcement, there was a slight increase in the number of inspectors general who reported that their agencies were not following these procedures. Six inspectors general noted that their agency was not following procedures for internal incident reporting compared to five in fiscal year 2007. Four inspectors general noted that their agency was not following reporting procedures to US-CERT compared to two in 2007, and two noted that their agency was not following reporting procedures to law enforcement compared to one in 2007.

At least 12 inspectors general also noted specific weaknesses in incident procedures such as a lack of fully documented policies and procedures for responding to security incidents, a lack of control procedures to ensure that audit trails were being maintained and reviewed, and instances where incidents were not always handled and reported in accordance with requirements. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Without proper incident response and documentation, agencies risk losing valuable information needed to prevent future exploits and to understand the nature and cost of the threats directed at them.

Agencies Report Improvements in Remedial Actions, but Processes Could Be Strengthened

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. In addition, OMB requires agencies to report quarterly regarding their remediation efforts for all programs and systems where a security weakness has been identified. It also requests that inspectors general assess and report annually on whether their agency has developed, implemented, and managed an agencywide process for these plans.

Inspectors general reported an increase in the number of agencies that had developed and implemented plans of action and milestones (POA&M) when weaknesses were identified. For 2008, 13 inspectors general reported that their agency had developed POA&Ms 96 to 100 percent of the time when weaknesses were identified; up from 11 inspectors general reporting this in 2007. However, many still cited weaknesses with their agency's POA&M process. Several mentioned that their agency did not always include weaknesses or vulnerabilities identified through security controls testing or inspector general reviews in the POA&M. They also reported that their agency did not always properly track weaknesses because the status of individual weaknesses was not always accurate. Without a sound remediation process, agencies cannot be assured that information security weaknesses have been efficiently and effectively corrected.

Inspectors General Report Using Professional Standards for Conducting Independent Evaluations More, but Opportunities to Improve Consistency Remain

An increasing number of inspectors general reported conducting annual independent evaluations in accordance with professional standards and provided additional information about the effectiveness of their agency's security programs. FISMA requires agency inspectors general or their independent external auditors to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of the programs and practices. We have previously reported[23] that the annual inspector general independent evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. We noted that there was an opportunity to improve these evaluations by conducting them in accordance with audit standards or a common approach and framework.

In fiscal year 2008, 16 of 24 inspectors general cited using professional standards to perform the annual FISMA evaluations, up from 8 inspectors general who cited using standards the previous year. Of the 16 inspectors general, 13 reported performing evaluations that were in accordance with generally accepted government auditing standards, while the other 3 indicated using the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.[24] The remaining eight inspectors general cited using internally developed standards or did not indicate whether they had performed their evaluations in accordance with professional standards.

In addition, an increasing number of inspectors general provided supplemental information about their agency's information security policies and practices. To illustrate, 21 of 24 inspectors general reported additional information about the effectiveness of their agency's security controls and programs that was above and beyond what was requested in the OMB template, an increase from the 18 who had provided such additional information in their fiscal year 2007 reports. The additional information included descriptions of significant control deficiencies and

[23] GAO-07-837 and GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: Mar. 12, 2008).

[24] 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 inspector general personnel throughout government. The Inspector General Reform Act of 2008 combined the council with the Executive Council on Integrity and Efficiency to create the Council of Inspectors General on Integrity and Efficiency.

weaknesses in security processes that provided additional context to the agency's security posture.

Although inspectors general reported using professional standards more frequently, their annual independent evaluations occasionally lacked consistency. For example,

- Three inspectors general provided only template responses and did not identify the scope and methodology of their evaluation. (These three inspectors general were also among those who had not reported performing their evaluation in accordance with professional standards.)

- Descriptions of the controls evaluated during the review as documented in the scope and methodology sections differed. For example, according to their FISMA reports, a number of inspectors general stated that their evaluations included a review of policies and procedures, whereas others did not indicate whether policies and procedures had been reviewed. Additionally, multiple inspectors general also indicated that technical vulnerability assessments had been conducted as part of the review, whereas others did not indicate whether such an assessment had been part of the review.

- Eleven inspectors general indicated that their FISMA evaluations considered the results of previous information security reviews, whereas 13 inspectors general did not indicate whether they considered other information security work, if any.

The development and use of a common framework or adherence to auditing standards could provide improved effectiveness, increased efficiency, quality control, and consistency in inspector general assessments.

Opportunities Remain for OMB to Improve Annual Reporting and Oversight of Agency Information Security Programs

Although OMB has supported several governmentwide initiatives and provided additional guidance to help improve information security at agencies, opportunities remain for it to improve its annual reporting and oversight of agency information security programs. FISMA specifies that OMB, among other responsibilities, is to develop policies, principles, standards, and guidelines on information security and report to Congress not later than March 1 of each year on agencies' implementation of FISMA. Each year, OMB provides instructions to federal agencies and their inspectors general for preparing their FISMA reports and then summarizes the information provided by the agencies and the inspectors general in its report to Congress.

Over the past 4 years, we have reported[25] that, while the 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, shortcomings in OMB's reporting instructions limited the utility of the annual reports. Accordingly, we recommended that OMB improve reporting by clarifying reporting instructions; develop additional metrics that measure control effectiveness; request inspectors general to assess the quality of additional information security processes such as system test and evaluation, risk categorization, security awareness training, and incident reporting; and require agencies to report on additional key security activities such as patch management. Although OMB has taken some actions to enhance its reporting instructions, it has not implemented most of the recommendations, and thus further actions need to be taken to fully address them.

In addition to the previously reported shortcomings, OMB's reporting instructions for fiscal year 2008 did not sufficiently address several processes key to implementing an agencywide security program and were sometimes unclear. For example, the reporting instructions did not request inspectors general to provide information on the quality or effectiveness of agencies' processes for developing and maintaining inventories, providing specialized security training, and monitoring contractors. For these activities, inspectors general were requested to report only on the extent to which agencies had implemented the activity but not on the effectiveness of those activities. Providing information on the effectiveness of the processes used to implement the activities could further enhance the usefulness of the data for management and oversight purposes.

OMB's guidance to inspectors general for rating agencies' certification and accreditation processes was not clear. In its reporting instructions, OMB requests inspectors general to rate their agency's certification and accreditation process using the terms "excellent," "good," "satisfactory,"

[25] GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005); GAO-07-837; and GAO-08-571T.

"poor," or "failing." However, the reporting instructions do not define or identify criteria for determining the level of performance for each rating. OMB also requests inspectors general to identify the aspect(s) of the certification and accreditation process they included or considered in rating the quality of their agency's process. Examples OMB included were security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, and security configurations (including patch management). While this information is helpful and provides insight on the scope of the rating, inspectors general were not requested to comment on the quality or effectiveness of these items. Additionally, not all inspectors general considered the same aspects in reviewing the certification and accreditation process, yet all were allowed to provide the same rating. Without clear guidelines for rating these processes, OMB and Congress may not have a consistent basis for comparing the progress of an agency over time or against other agencies.

In its report to Congress for fiscal year 2008, OMB did not fully summarize the findings from the inspectors general independent evaluations or identify significant deficiencies in agencies' information security practices. FISMA requires OMB to provide a summary of the findings of agencies' independent evaluations and significant deficiencies in agencies' information security practices. Inspectors general often document their findings and significant information security control deficiencies in reports that support their evaluations. However, OMB did not summarize and present this information in its annual report to Congress. Most of the inspectors general information summarized in the annual report was taken from the "yes" or "no" responses or from questions having a predetermined range of percentages as stipulated by OMB's reporting template. Thus, important information about the implementation of agency information security programs and the vulnerabilities and risks associated with federal information systems was not provided to Congress in OMB's annual report. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices. As a result, Congress may not be fully informed about the state of federal information security.

OMB also did not approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually and approve or disapprove them. OMB representatives informed us that they review agencies' FISMA reports and interact with agencies whenever an issue arises that requires their oversight. However, representatives stated that they do not explicitly or publicly declare that an agency's information security program has been approved or disapproved. As a result, a mechanism for establishing accountability and holding agencies accountable for implementing effective programs was not used.

Conclusions

Weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of the sensitive data maintained by federal agencies. These weaknesses, including those for access controls, configuration management, and segregation of duties, leave federal agency systems and information vulnerable to external as well as internal threats. The White House, OMB, and federal agencies have initiated actions intended to enhance information security at federal agencies. However, until agencies fully and effectively implement information security programs and address the hundreds of recommendations that we and agency inspectors general have made, federal systems will remain at an increased and unnecessary risk of attack or compromise.

Despite these weaknesses, federal agencies have continued to report progress in implementing key information security requirements. While NIST, inspectors general, and OMB have all made progress toward fulfilling their statutory requirements, the current reporting process does not produce information to accurately gauge the effectiveness of federal information security activities. OMB's annual reporting instructions did not cover key security activities and were not always clear. Finally, OMB did not include key information about findings and significant deficiencies identified by inspectors general in its governmentwide report to Congress and did not approve or disapprove agency information security programs. Shortcomings in reporting and oversight can result in insufficient information being provided to Congress and diminish its ability to monitor and assist federal agencies in improving the state of federal information security.

Recommendations for Executive Action

We recommend that the Director of the Office of Management and Budget take the following four actions:

- Update annual reporting instructions to request inspectors general to report on the effectiveness of agencies' processes for developing inventories, monitoring contractor operations, and providing specialized security training.

- Clarify and enhance reporting instructions to inspectors general for certification and accreditation evaluations by providing them with guidance on the requirements for each rating category.

- Include in OMB's report to Congress, a summary of the findings from the annual independent evaluations and significant deficiencies in information security practices.

- Approve or disapprove agency information security programs after review.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Federal Chief Information Officer (CIO)[26] generally agreed with our overall assessment of information security at the agencies. He also identified actions that OMB is taking to clarify its reporting guidance and to consider more effective security performance metrics. These actions are consistent with the intent of two of our recommendations, that OMB clarify and enhance reporting instructions and request inspectors general to report on additional measures of effectiveness.

The Federal CIO did not address our recommendation to include a summary of the findings and significant security deficiencies in its report to Congress and did not concur with GAO's conclusion that OMB does not approve or disapprove agencies' information security management programs on an annual basis. He indicated that OMB reviews all agency and IG FISMA reports annually; reviews quarterly information on the major agencies' security programs; and uses this information, and other reporting, to evaluate agencies security programs. The Federal CIO advised that concerns are communicated directly to the agencies. We acknowledge that these are important oversight activities. However, as we reported, OMB did not demonstrate that it approved or disapproved agency information security programs, as required by FISMA. Consequently, a mechanism for holding agencies accountable for implementing effective programs is not being effectively used.

[26] On March 5, 2009, the President named a Federal Chief Information Officer at the White House to direct the policy and strategic planning of federal information technology investments and be responsible for oversight of federal technology spending. The Federal CIO also establishes and oversees enterprise architecture to ensure system interoperability and information sharing and ensure information security and privacy across the federal government.

We are sending copies of this report to the Office of Management and Budget and other interested parties. 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 IV.

Gregory C. Wilshusen

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 2007 through April 2009. We also reviewed and analyzed the information security work and products of agency inspectors general. Further, we reviewed and summarized weaknesses identified in our reports and that of inspectors general using five major categories of information security controls: (1) access controls, (2) configuration management controls, (3) segregation of duties, (4) continuity of operations planning, and (5) agencywide information security programs. Our reports generally used the methodology contained in the *Federal Information System Controls Audit Manual.*[1] We also examined information provided by the U.S. Computer Emergency Readiness Team (US-CERT) on reported security incidents.

To assess the implementation of FISMA requirements, we reviewed and analyzed the provisions of the act[2] and the mandated annual FISMA reports from the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the CIOs and IGs of 24 major federal agencies for fiscal years 2007 and 2008. We also examined OMB's FISMA reporting instructions and other OMB and NIST guidance.

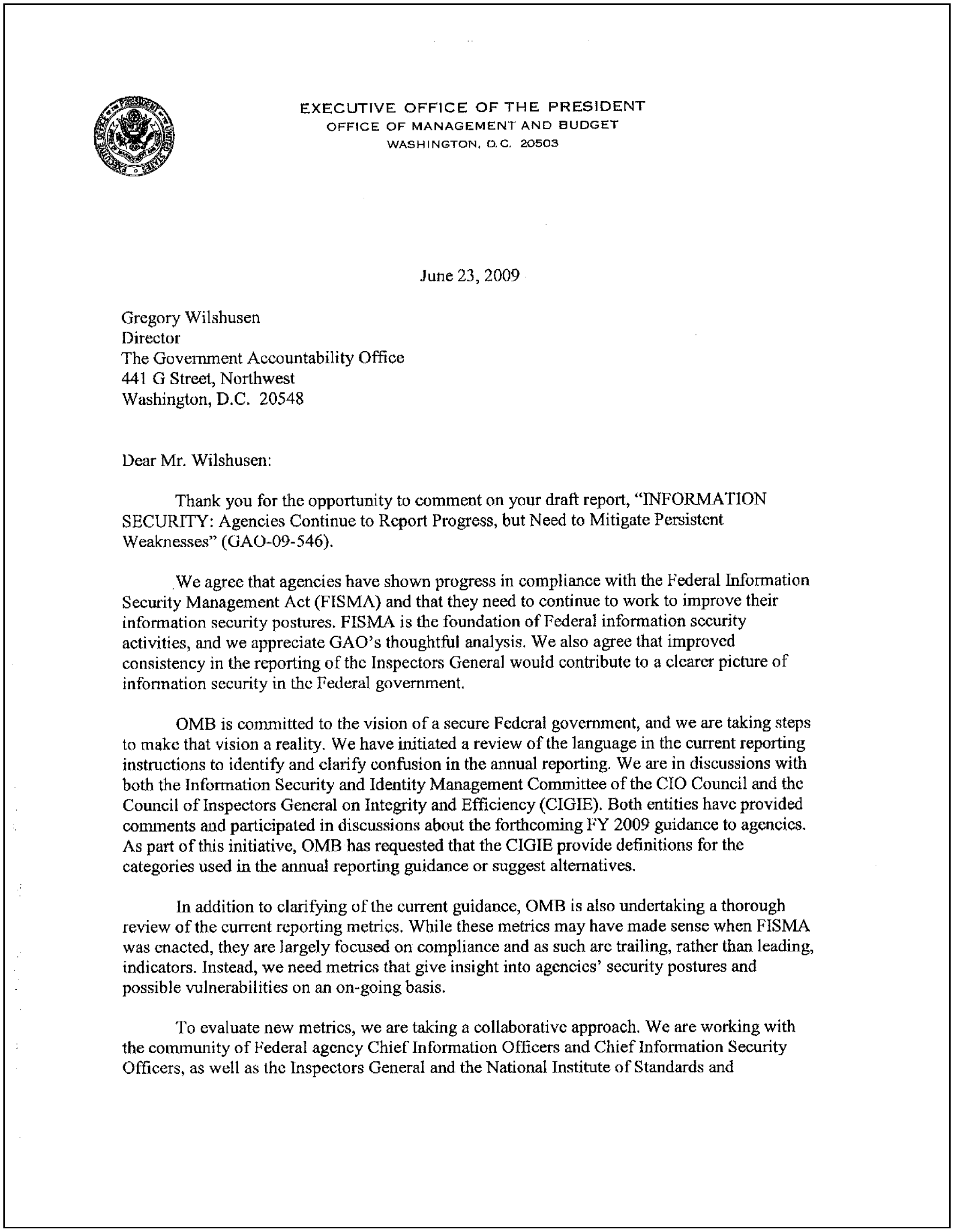
We also held discussions with OMB representatives and agency officials from the National Institute of Standards and Technology and the Department of Homeland Security's US-CERT to further assess the implementation of FISMA requirements. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to corroborate information provided in their responses. 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.

[1] GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

[2] Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

We conducted this performance audit from December 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Office of Management and Budget



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

June 23, 2009

Gregory Wilshusen
Director
The Government Accountability Office
441 G Street, Northwest
Washington, D.C. 20548

Dear Mr. Wilshusen:

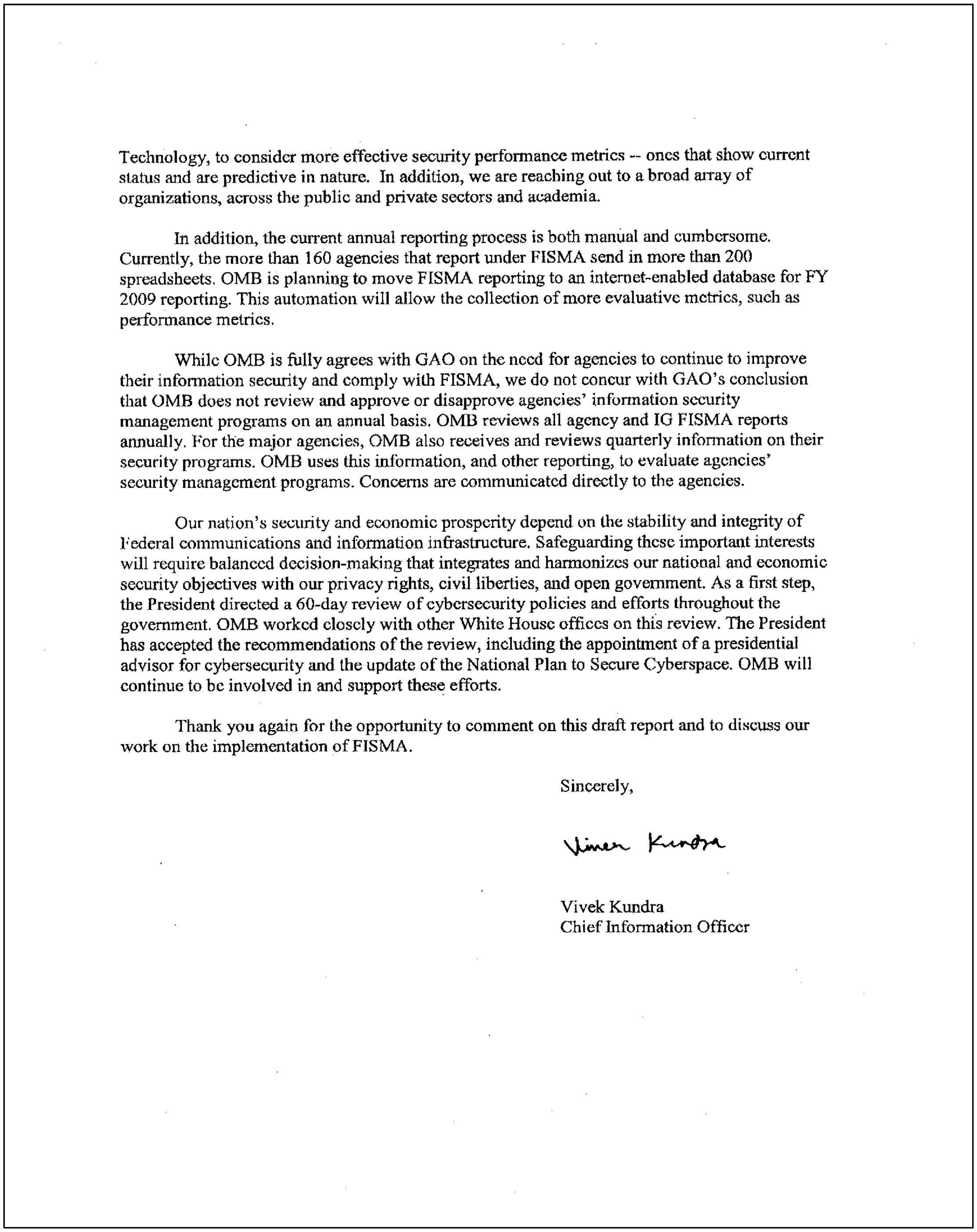
Thank you for the opportunity to comment on your draft report, "INFORMATION SECURITY: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses" (GAO-09-546).

We agree that agencies have shown progress in compliance with the Federal Information Security Management Act (FISMA) and that they need to continue to work to improve their information security postures. FISMA is the foundation of Federal information security activities, and we appreciate GAO's thoughtful analysis. We also agree that improved consistency in the reporting of the Inspectors General would contribute to a clearer picture of information security in the Federal government.

OMB is committed to the vision of a secure Federal government, and we are taking steps to make that vision a reality. We have initiated a review of the language in the current reporting instructions to identify and clarify confusion in the annual reporting. We are in discussions with both the Information Security and Identity Management Committee of the CIO Council and the Council of Inspectors General on Integrity and Efficiency (CIGIE). Both entities have provided comments and participated in discussions about the forthcoming FY 2009 guidance to agencies. As part of this initiative, OMB has requested that the CIGIE provide definitions for the categories used in the annual reporting guidance or suggest alternatives.

In addition to clarifying of the current guidance, OMB is also undertaking a thorough review of the current reporting metrics. While these metrics may have made sense when FISMA was enacted, they are largely focused on compliance and as such are trailing, rather than leading, indicators. Instead, we need metrics that give insight into agencies' security postures and possible vulnerabilities on an on-going basis.

To evaluate new metrics, we are taking a collaborative approach. We are working with the community of Federal agency Chief Information Officers and Chief Information Security Officers, as well as the Inspectors General and the National Institute of Standards and



Technology, to consider more effective security performance metrics -- ones that show current status and are predictive in nature. In addition, we are reaching out to a broad array of organizations, across the public and private sectors and academia.

In addition, the current annual reporting process is both manual and cumbersome. Currently, the more than 160 agencies that report under FISMA send in more than 200 spreadsheets. OMB is planning to move FISMA reporting to an internet-enabled database for FY 2009 reporting. This automation will allow the collection of more evaluative metrics, such as performance metrics.

While OMB is fully agrees with GAO on the need for agencies to continue to improve their information security and comply with FISMA, we do not concur with GAO's conclusion that OMB does not review and approve or disapprove agencies' information security management programs on an annual basis. OMB reviews all agency and IG FISMA reports annually. For the major agencies, OMB also receives and reviews quarterly information on their security programs. OMB uses this information, and other reporting, to evaluate agencies' security management programs. Concerns are communicated directly to the agencies.

Our nation's security and economic prosperity depend on the stability and integrity of Federal communications and information infrastructure. Safeguarding these important interests will require balanced decision-making that integrates and harmonizes our national and economic security objectives with our privacy rights, civil liberties, and open government. As a first step, the President directed a 60-day review of cybersecurity policies and efforts throughout the government. OMB worked closely with other White House offices on this review. The President has accepted the recommendations of the review, including the appointment of a presidential advisor for cybersecurity and the update of the National Plan to Secure Cyberspace. OMB will continue to be involved in and support these efforts.

Thank you again for the opportunity to comment on this draft report and to discuss our work on the implementation of FISMA.

Sincerely,

Vivek Kundra

Vivek Kundra
Chief Information Officer

Appendix III: Cybersecurity Experts Highlighted Key Improvements for Strengthening the Nation's Cyber Security

In March 2009, we convened a panel of experts to discuss how to improve key aspects of the national cyber security strategy and its implementation as well as other critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private-sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cyber security posture. These improvements are in large part consistent with our previously mentioned reports and extensive research and experience in this area.

Table 2: Key Improvements Needed to Strengthen the Nation's Cybersecurity Posture

Cyber security improvement	Description
1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.	The strategy should, among other things, (1) include well-defined strategic objectives, (2) provide understandable goals for the government and the private sector (end game), (3) articulate cyber priorities among the objectives, (4) provide a vision of what a secure cyber space should be in the future, (5) seek to integrate federal government capabilities, (6) establish metrics to gauge whether progress is being made against the strategy, and (7) provide an effective means for enforcing action and accountability when there are progress shortfalls. According to expert panel members, the CNCI provides a good set of tactical initiatives focused on improving primarily federal cyber security; however, it does not provide strategic objectives, goals, and priorities for the nation as a whole.
2. Establish White House responsibility and accountability for leading and overseeing national cyber security policy.	The strategy makes the Department of Homeland Security (DHS) the focal point for cyber security; however, according to expert panel members, DHS has not met expectations and has not provided the high-level leadership needed to raise cyber security to a national focus. Accordingly, panelists stated that to be successful and to send the message to the nation and cyber critical infrastructure owners that cyber security is a priority, this leadership role needs to be elevated to the White House. In addition, to be effective, the office must have, among other things, commensurate authority— for example, over budgets and resources—to implement and employ incentives that will encourage action.
3. Establish a governance structure for strategy implementation.	The strategy establishes a public/private partnership governance structure that includes 18 critical infrastructure sectors, corresponding government and sector coordinating councils, and cross-sector councils. However, according to panelists, this structure is government-centric and largely relies on personal relationships to instill trust to share information and take action. In addition, although all sectors are not of equal importance in regard to their cyber assets and functions, the structure treats all sectors and all critical cyber assets and functions equally. To ensure effective strategy implementation, experts stated that the partnership structure should include a committee of senior government representatives (for example, the Departments of Defense, Homeland Security, Justice, State, and the Treasury and the White House) and private-sector leaders representing the most critical cyber assets and functions. Expert panel members also suggested that this committee's responsibilities should include measuring and periodically reporting on progress in achieving the goals, objectives, and strategic priorities established in the national strategy and building consensus to hold involved parties accountable when there are progress shortfalls.

Cyber security improvement	Description
4. Publicize and raise awareness about the seriousness of the cyber security problem.	Although the strategy establishes cyberspace security awareness as a priority, experts stated that many national leaders in business and government, including in Congress, who can invest resources to address cyber security problems are generally not aware of the severity of the risks to national and economic security posed by the inadequacy of our nation's cyber security posture and the associated intrusions made more likely by that posture. Expert panel members suggested that an aggressive awareness campaign is needed to raise the level of knowledge of leaders and the general populace that protecting our information and systems from cyber attack is ongoing.
5. Create an accountable, operational cyber security organization.	DHS established the National Cyber Security Division (within the Office of Cybersecurity and Communications) to be responsible for leading national day-to-day cyber security efforts; however, according to panelists, this has not enabled DHS to become the national focal point as envisioned. Panel members stated that currently the Department of Defense and other organizations within the intelligence community that have significant resources and capabilities have come to dominate federal efforts. They told us that there also needs to be an independent cyber security organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and the nation's international allies to address incidents against the nation's critical cyber systems and functions. However, there was not a consensus among our expert panel members regarding where this organization should reside.
6. Focus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.	The strategy recommends actions to identify critical cyber assets and functions, but panelists stated that efforts to identify which cyber assets and functions are most critical to the nation have been insufficient. According to panel members, inclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence. In addition, the current strategy establishes vulnerability reduction as a key priority; however, according to panelists, efforts to identify and mitigate known vulnerabilities have been insufficient. They stated that greater efforts should be taken to identify and eliminate common vulnerabilities and that there are techniques available that should be used to assess vulnerabilities in the most critical, prioritized cyber assets and functions.
7. Bolster public/private partnerships through an improved value proposition and use of incentives.	While the strategy encourages action by owners and operators of critical cyber assets and functions, panel members stated that there are not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering in cyber security. Accordingly, panelists stated that the federal government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cyber security-related resources.
8. Focus greater attention on addressing the global aspects of cyberspace.	The strategy includes recommendations to address the international aspects of cyber space but, according to panelists, the United States is not addressing global issues impacting how cyber space is governed and controlled. They added that, while other nations are actively involved in developing treaties, establishing standards, and pursuing international agreements (such as on privacy), the United States is not aggressively working in a coordinated manner to ensure that international agreements are consistent with U.S. practice and that they address cyber security and cyber crime considerations. Panel members stated that the United States should pursue a more coordinated, aggressive approach so that there is a level playing field globally for U.S. corporations and enhanced cooperation among government agencies, including law enforcement. In addition, a panelist stated that the United States should work towards building consensus on a global cyber strategy.

Cyber security improvement	Description
9. Improve law enforcement efforts to address malicious activities in cyberspace.	The strategy calls for improving investigative coordination domestically and internationally and promoting a common agreement among nations on addressing cyber crime. According to one panelist, some improvements in domestic law have been made (e.g., enactment of the PROTECT Our Children Act of 2008), but implementation of this act is a work-in-process due to its recent passage. Panel members also stated that current domestic and international law enforcement efforts, including activities, procedures, methods, and laws are too outdated and outmoded to adequately address the speed, sophistication, and techniques of individuals and groups, such as criminals, terrorists, and others who have malicious intent. Improved law enforcement is essential to more effectively catch and prosecute malicious individuals and groups and, with stricter penalties, deter malicious behavior.
10. Place greater emphasis on cyber security research and development, including consideration of how to better coordinate government and private-sector efforts.	While the strategy recommends actions to develop a research and development agenda and coordinate efforts between the government and private sector, experts stated that the United States is not adequately focusing and funding research and development efforts to address cyber security or to develop the next generation of cyber space to include effective security capabilities. In addition, the research and development efforts currently under way are not being well coordinated between government and the private sector.
11. Increase the cadre of cyber security professionals.	The strategy includes efforts to increase the number and skills of cyber security professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cyber crime investigators. Expert panel members stated that actions to increase the number of professionals with adequate cyber security skills should include (1) enhancing existing scholarship programs (e.g., Scholarship for Service) and (2) making the cyber security discipline a profession through testing and licensing.
12. Make the federal government a model for cyber security, including using its acquisition function to enhance cyber security aspects of products and services.	The strategy establishes securing the government's cyber space as a key priority and advocates using federal acquisition to accomplish this goal. Although the federal government has taken steps to improve the cyber security of agencies (e.g., beginning to implement the CNCI initiatives), panelists stated that it still is not a model for cyber security. Further, they said the federal government has not made changes in its acquisition function and the training of government officials in a manner that effectively improves the cyber security capabilities of products and services purchased and used by federal agencies.

Source: GAO.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Charles Vrabel (Assistant Director); Debra Conner; Larry Crosland; Sharhonda Deloach; Neil Doherty; Kristi Dorsey; Rosanna Guererro; Nancy Glover; Rebecca Eyler; Mary Marshall; and Jayne Wilson made key contributions to this report.

Related GAO Products

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System. GAO-09-355. Washington, D.C.: June 1, 2009.

Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. GAO-09-292. Washington, D.C.: May 13, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

Freedom of Information Act: DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness. GAO-09-260. Washington, D.C.: March 20, 2009.

Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls. GAO-09-203. Washington, D.C.: March 16, 2009.

National Cyber Security Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data. GAO-09-195. Washington, D.C.: January 30, 2009.

Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS. GAO-09-136. Washington, D.C.: January 9, 2009.

Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements. GAO-08-1180T. Washington, D.C.: September 25, 2008.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cyber Security Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network. GAO-08-1001. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Information Security: FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems. GAO-08-564. Washington, D.C.: May 30, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Information Security: TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks. GAO-08-775T. Washington, D.C.: May 21, 2008.

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. GAO-08-571T. Washington, D.C.: March 12, 2008.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. GAO-08-280. Washington, D.C.: February 29, 2008.

Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies. GAO-08-496T. Washington, D.C.: February 14, 2008.

Information Security: Protecting Personally Identifiable Information. GAO-08-343. Washington, D.C.: January 25, 2008.

Information Security: IRS Needs to Address Pervasive Weaknesses. GAO-08-211. Washington, D.C.: January 8, 2008.

Veterans Affairs: Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and

Strengthening Information Security. GAO-07-1264T. Washington, D.C.: September 26, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs. GAO-07-1019. Washington, D.C.: September 7, 2007.

Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements. GAO-07-528. Washington, D.C.: August 31, 2007.

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

Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program. GAO-07-870. Washington, D.C.: July 13, 2007.

Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program. GAO-07-1003T. Washington, D.C.: June 20, 2007.

Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk. GAO-07-935T. Washington, D.C.: June 7, 2007.

Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program. GAO-07-351. Washington, D.C.: May 18, 2007.

(311020)

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

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

Public Affairs

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