United States Government Accountability Office

GAO

Testimony Before the
Subcommittee on Government Management,
Organization, and Procurement,
Committee on Oversight and Government Reform,
U.S. House of Representatives

For Release on Delivery
Expected at 9:00 a.m. EDT
May 19, 2009

INFORMATION SECURITY

Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist

GAO-09-701T

May 19, 2009

INFORMATION SECURITY

Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-701T, a testimony before the House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Without proper safeguards, federal agencies' computer systems are vulnerable to intrusions by individuals and groups who have malicious intentions and can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Concerned by reports of significant weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on its draft report on (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) their implementation of FISMA requirements. To prepare for this testimony, GAO summarized its draft report where it analyzed agency, inspectors general, Office of Management and Budget (OMB), congressional, and GAO reports on information security.

What GAO Recommends

In its draft report, GAO is recommending that the Director of OMB take several actions, including revising guidance.

View GAO-09-701T or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Significant weaknesses in information security policies and practices expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. GAO's audits and reviews by inspectors general note significant information security control deficiencies that place agency operations and assets at risk. In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that the information system controls over their financial systems and information were either a significant deficiency or a material weakness. In addition, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. Twenty-three of the 24 major federal agencies had weaknesses in their agencywide information security programs.

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. For fiscal year 2008 reporting, agencies reported higher levels of FISMA implementation for most information security metrics and lower levels for others. Increases were reported in the number and percentage of employees and contractors receiving security awareness training, the number and percentage of systems with tested contingency plans, and the number and percentage of systems that were certified and accredited. However, the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly and the number and percentage of systems that had been tested and evaluated at least annually decreased slightly. In addition, the current reporting instructions do not request inspectors general to report on agencies' effectiveness of key activities and did not always provide them with clear guidance for annual reporting. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices. Without such information, Congress may not be fully informed about the state of federal information security.

Chairwoman Watson and Members of the Subcommittee:

Thank you for inviting me to discuss our work on federal agencies' implementation of information security policies and practices under the Federal Information Security Management Act of 2002 (FISMA).[1] Information security is a critical consideration for any federal department or agency, where information systems and computer networks are used to carry out its mission and where maintaining 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.

Without proper safeguards, federal agencies' computer systems are vulnerable to intrusions by individuals and groups with malicious intentions who can obtain 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. Over the past few years, the 24 major federal agencies[2] 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 the loss of privacy, identity theft, and other financial crimes.

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

[2]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.

Concerned by reports of significant weaknesses in federal systems, Congress passed FISMA in 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. Six years after FISMA was enacted, we continue to report that poor information security is a widespread problem with potentially devastating consequences. Moreover, since 1997, we have identified information security as a governmentwide high-risk issue in our biennial reports to Congress.[3]

In my testimony today, I will summarize the results of our review of (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) agencies' implementation of FISMA. We currently have a draft report providing additional detail on that review that we will be finalizing and issuing publicly at a later date. In conducting our review, we analyzed agency, inspector general, Office of Management and Budget (OMB), congressional, and our reports on information security. We conducted the review from December 2008 to May 2009 in the Washington, D.C., area in accordance with generally accepted government auditing standards.

After a brief summary of the laws and guidance currently in place, my remarks will focus on the results of our review.

Background

FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its 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[4]—assessing risk, establishing a central management focal point, implementing appropriate policies

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

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

and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to agency heads, chief information officers, inspectors general, and the National Institute for Science and Technology (NIST). It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing, at least annually, and approving or disapproving, agency information security programs.

Federal Law and Policy Established Federal Information Security Requirements

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

- periodic assessments of the risk that could result from the compromise of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;

- procedures for detecting, reporting, and responding to security incidents;
- plans and procedures to ensure continuity of operations; and
- an annually updated inventory of major information systems operated by the agency or under its control.

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.

NIST, agency inspectors general, and OMB also play key roles under FISMA. NIST, for example, is required to provide standards and guidance to agencies on information security. In addition, NIST is tasked with developing 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. NIST has issued guidance through its FISMA Implementation Project and has expanded its work through other security activities. In addition, NIST's computer security division issued its 2008 annual report, as mandated by FISMA. Agency inspectors general are required to perform an independent annual evaluation of the agency's information security program and practices. These reviews should include testing of information security procedures policies and practices for a representative subset of agency systems, as well as an assessment of compliance with FISMA and any related information security policies, procedures, standards, and guidelines.

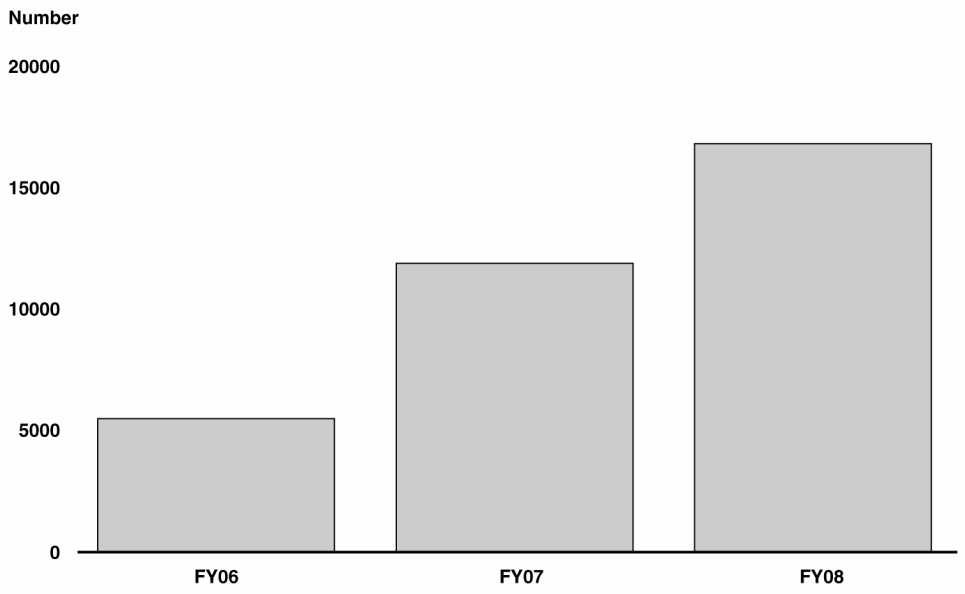
FISMA also requires OMB to develop policies, principles, standards, and guidelines on information security and is required to report annually to Congress on agency compliance with the requirements

of the act. OMB has provided instructions to federal agencies and their inspectors general for preparing annual FISMA reports. OMB's reporting instructions focus on performance metrics related to the performance of key control activities such as developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, testing contingency plans, and certifying and accrediting systems.

Weaknesses in Information Security Controls Place Sensitive Information at Risk

Significant weaknesses in information security policies and practices expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. 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. When incidents occur, agencies are to notify the federal information security incident center—US-Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

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

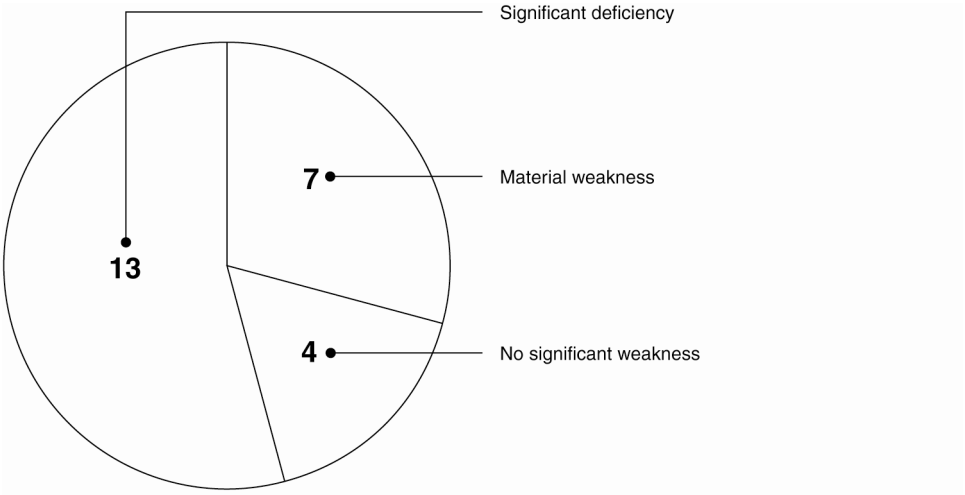


Source: GAO analysis of US-CERT data.

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 24 major agencies noted that their information system controls over their financial systems and information were either a material weakness or a significant deficiency[5] (see fig. 2).

[5]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 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2008.

Agency inspectors general have also reported weaknesses in information security, with 22 of 24 identifying information security as a "major management challenge" for their agency.[6]

Over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, our analysis of inspector general, agency, and our own reports reveals that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. Weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. Agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply

[6]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).

encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. At least nine agencies also lacked effective controls to restrict physical access to information assets. We have previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information necessary to restore services in a timely manner. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. 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. Twenty-three of the 24 major federal agencies had weaknesses in their agencywide information security programs. Due to the persistent nature of information security vulnerabilities and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress;[7] a designation we have made in each report since 1997.

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

Enhancements Can Be Made to Strengthen Federal Information Security

Over the past several years, we and agency 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 contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings 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.

In addition, the White House, OMB, and some federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. They include the Comprehensive National Cyber Security Initiative, the Information Systems Security Line of Business, the Federal Desktop Core Configuration, SmartBUY, and the Trusted Internet Connections Initiative. We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

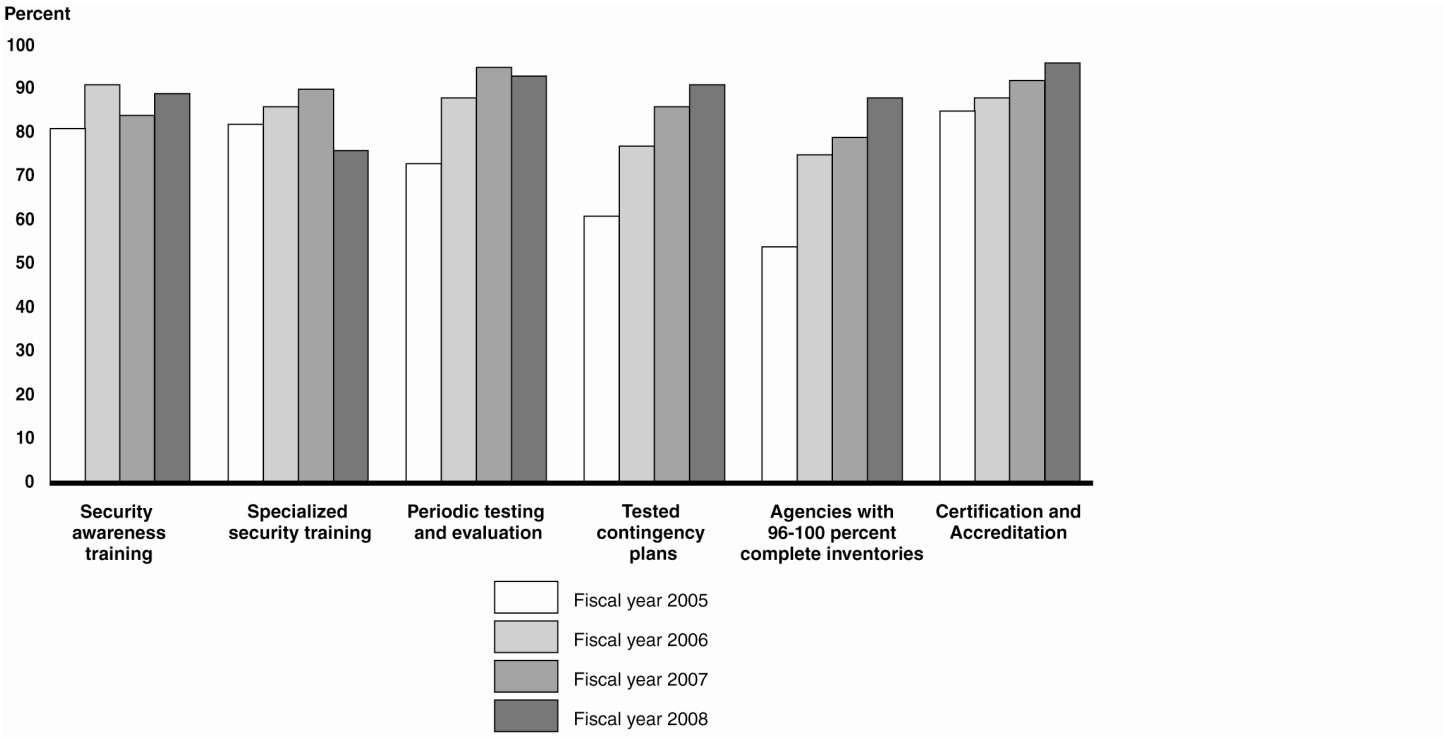
Agencies Continue to Report Progress in Implementing Requirements

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,[8] 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 (from 95 percent in fiscal year 2007 to 93 percent in fiscal year 2008) and the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly (from 90 percent in fiscal year 2007 to 76 percent in 2008). (See fig 3.)

[8]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 3: Selected Performance Metrics for Agency Systems



Source: GAO analysis of IG and agency data.

Most Inspectors General Cite the Use of Professional Standards for Evaluation

FISMA requires agency inspectors general to perform an independent evaluation of the information security programs and practices of their agency to determine the effectiveness of such programs and practices. Each evaluation is to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assessing compliance (based on the results of the testing) with FISMA requirements and related information security policies, procedures, standards, and guidelines.

We have previously reported[9] that the annual inspector general independent evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. We stated that there was an opportunity to improve these evaluations by conducting them in accordance with audit standards or a common approach and framework. In their 2008 FISMA reports, more inspectors general indicated using professional standards (16) than had in their 2007 reports (8); in addition, 21 of 24 provided supplemental information about the agency's implementation of FISMA. 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.

OMB Can Improve Annual Reporting and Oversight of Agencies' Information Security Programs

FISMA specifies that OMB is to develop policies, principles, standards, and guidelines on information security. Each year, OMB provides instructions to federal agencies and their inspectors general for FISMA annual reporting. Additionally, OMB summarizes the information provided by the agencies and the inspectors general in its report to Congress. We have previously made several recommendations to OMB for improving this annual reporting. OMB has required agencies to report systems information by risk category and reviewed its guidance to ensure clarity of instructions.

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

[9]GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July, 2007) and *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: March 12, 2008).

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.

In addition, the guidance to inspectors general did not define or identify criteria for determining the level of performance in certification and accreditation for each rating. 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. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices.

OMB also did not explicitly approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually, and approve or disapprove them. As a result, a mechanism for establishing accountability and holding agencies accountable for implementing effective programs was not used.

– – – –

In summary, as illustrated by recent incidents at federal agencies, significant weaknesses in information security policies and practices expose sensitive data to significant risk. Almost all major agencies reported weaknesses in one or more areas of information security controls during fiscal year 2008. Despite these persistent weaknesses, agencies reported increased compliance in implementing key information security activities. While the

inspectors general and OMB have made progress toward fulfilling their statutory requirements, OMB's annual reporting instructions did not cover key security activities and were not always clear. In addition, 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 or misleading information being provided to Congress and diminish its ability to monitor and assist federal agencies in improving the state of federal information security.

Chairwoman Watson, this concludes my statement. I would be happy to answer any questions you or other members of the subcommittee may have.

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Charles Vrabel (Assistant Director), Larry Crosland, Neil Doherty, Nancy Glover, and Jayne Wilson.