United States Government Accountability Office

GAO

Report to Congressional Committees

July 2005

# INFORMATION SECURITY

# Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements


GAO-05-552

July 2005

# INFORMATION SECURITY

# Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-552, a report to congressional committees

## Why GAO Did This Study

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002.

In accordance with FISMA requirements that the Comptroller General report periodically to the Congress, GAO's objectives in this report are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the federal government's implementation of FISMA requirements.

## What GAO Recommends

GAO recommends that the Director of the Office of Management and Budget (OMB) implement improvements in the annual FISMA reporting guidance. In commenting on a draft of this report, OMB agreed with GAO's overall assessment of information security at agencies but disagreed with aspects of our recommendations to enhance its FISMA reporting guidance.

www.gao.gov/cgi-bin/getrpt?GAO-05-552.

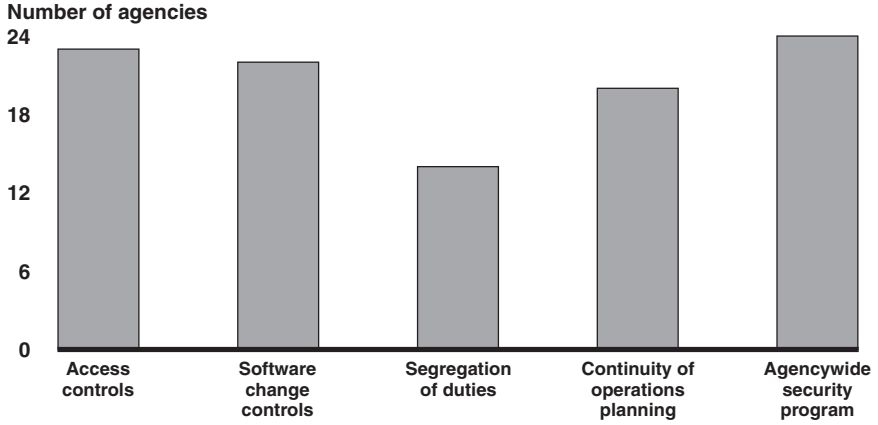
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

## What GAO Found

Pervasive weaknesses in the 24 major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of federal information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; continuity of operations planning was often inadequate; and security programs were not fully implemented at the agencies (see figure). These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Overall, the government is making progress in its implementation of FISMA. To provide a comprehensive framework for ensuring the effectiveness of information security controls, FISMA details requirements for federal agencies and their inspectors general (IG), the National Institute of Standards and Technology (NIST), and OMB. Federal agencies reported that they have been increasingly implementing required information security practices and procedures, although they continue to face major challenges. Further, IGs have conducted required annual evaluations, and NIST has issued required guidance in the areas of risk assessments and recommended information security controls, and has maintained its schedule for issuing remaining guidance required under FISMA. Finally, OMB has given direction to the agencies and reported to Congress as required; however, GAO's analysis of its annual reporting guidance identified opportunities to increase the usefulness of the reports for oversight. While progress has been made in implementing statutory requirements, agencies continue to have difficulty effectively protecting federal information and information systems.

**Information Security Weaknesses at the 24 Major Agencies**




Source: GAO.

# Contents

## Abbreviations

| | |
|---|---|
| CIO | chief information officer |
| DOD | Department of Defense |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act of 2002 |
| IG | Inspector General |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| US CERT | United States Computer Emergency Readiness Team |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, D.C. 20548**

July 15, 2005

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

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

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems through the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002.

FISMA recognizes that the major underlying cause for the majority of information security problems in federal agencies is the lack of an effective information security management program. Therefore, FISMA set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. In addition, FISMA provides a mechanism for improved oversight of federal agency information security programs. This mechanism includes mandated annual reporting by the agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). FISMA also includes a requirement for independent annual evaluations by the inspectors general (IG) or independent external auditors.

In accordance with the FISMA requirement that the Comptroller General report periodically to the Congress, our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) implementation of the FISMA requirements. To address

these objectives, we analyzed IG, agency, and GAO reports on information security. We conducted our evaluation from September 2004 through May 2005 in accordance with generally accepted government auditing standards. For further information about our objectives, scope, and methodology, refer to appendix I.

## Results in Brief

Federal agencies have not consistently implemented effective information security policies and practices. Pervasive weaknesses exist in almost all areas of information security controls at 24 major agencies, threatening the integrity, confidentiality, and availability of information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; and continuity of operations planning was often inadequate. These weaknesses exist because agencies have not yet fully implemented strong information security management programs. As a result, federal operations and assets are at increased risk of fraud, misuse, and destruction. In addition, these weaknesses place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Overall, the government is making progress in its implementation of the provisions of FISMA. To provide a comprehensive framework for ensuring the effectiveness of information security controls, FISMA details requirements for federal agencies and their IGs, NIST, and OMB. Federal agencies reported that they have been increasingly implementing required information security practices and procedures, although they continue to face major challenges. Further, IGs have conducted the required annual evaluations, and NIST has issued required guidance in the areas of risk assessments and information security controls and has maintained its schedule for issuing the remaining guidance required under FISMA. Finally, OMB has given direction to the agencies and reported to Congress as required; however, our analysis of the annual reporting guidance identified opportunities to increase the usefulness of the reports for oversight purposes. While progress has been made in implementing statutory requirements, agencies continue to have difficulty effectively protecting their information and information systems.

In our prior reports, as well as in reports by the IGs, specific recommendations were made to the agencies to remedy identified information security weaknesses. In this report, we recommend that OMB

take several actions to enhance its FISMA reporting guidance to agencies to increase the effectiveness and reliability of annual reporting.

In commenting on a draft of this report, OMB agreed with our overall assessment of information security at the agencies but disagreed with one of our recommendations to enhance its FISMA reporting guidance and provided comments on the others. OMB disagreed with our recommendation to ensure that all key FISMA requirements are reported on in annual reports and stated that reporting on additional sub-elements was not necessary. OMB also provided comments on actions it had or has taken related to the other recommendations. In addition, OMB provided other comments related to the contents of this report.

## Background

Federal agencies and our nation's critical infrastructures—such as power distribution, water supply, telecommunications, national defense, and emergency services—rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Protecting federal computer systems and the systems that support critical infrastructures has never been more important due to escalating threats of computer security incidents, the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks.

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. It is especially important for federal agencies where maintaining the public trust is essential. Without proper safeguards, there is enormous risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA permanently authorized and strengthened information security program, evaluation, and reporting requirements. It assigns specific responsibilities to agency heads and chief information officers (CIO), IGs, NIST, and OMB.

## 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, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency, through plans of action and milestones;[1]

[1]Plans of action and milestones are required for all programs and systems where an information technology security weakness has been found. The plan lists the weaknesses and shows estimated resource needs, or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

- 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.

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

Furthermore, FISMA established a requirement that each agency develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is to include 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.

**Responsibilities of the Inspectors General**

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

**Responsibilities of the National Institute of Standards and Technology**

Under FISMA, NIST is tasked with developing, for systems other than national security systems, (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 concerning detection and handling of information security incidents as well as guidelines, developed in conjunction with the Department of Defense (DOD) and the National Security Agency, for identifying an information system as a national security system.

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

- providing technical assistance to agencies on such elements as compliance with the standards and guidelines and the detection and handling of information security incidents;
- evaluating private-sector information security policies and practices and commercially available information technologies to assess potential application by agencies;
- evaluating security policies and practices developed for national security systems to assess their potential application by agencies; and
- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.

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

**Responsibilities of the Office of Management and Budget**

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

- developing and overseeing the implementation of policies, principles, standards, and guidelines on information security;
- requiring agencies to identify and provide information security protections commensurate with risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by

or on behalf of an agency, or information systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency;

- coordinating information security policies and procedures with related information resource management policies and procedures;
- overseeing agency compliance with FISMA to enforce accountability; and
- reviewing at least annually, and approving or disapproving, agency information security programs.

In addition, the act requires that OMB report to Congress no later than March 1 of each year on agency compliance with FISMA.

## Pervasive Weaknesses in Federal Agencies' Information Security Policies and Practices Place Data at Risk

The 24 major federal agencies[2] continue to have significant control weaknesses in their computer systems that threaten the integrity, confidentiality, and availability of federal information and systems. In addition, these weaknesses place financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

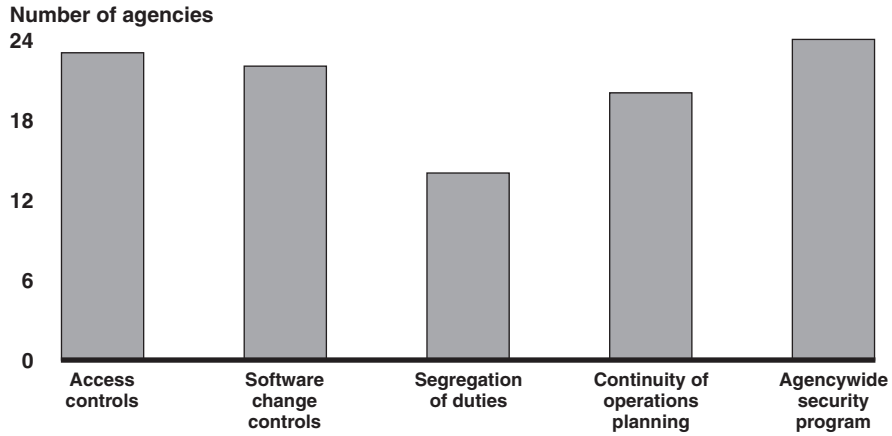
The weaknesses appear in the five major categories of information system controls (see fig. 1) defined in our audit methodology for performing information security evaluations and audits.[3] These areas are (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) software change controls, which provide assurance that only authorized software programs are implemented; (3) segregation of

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

[3]GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999). This methodology is used for our information security controls evaluations and audits, as well as by the IGs for the information security control work done as part of financial audits at the agencies.

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 security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

**Figure 1: Information Security Weaknesses at the 24 Major Agencies for Fiscal Year 2004**




Source: GAO.

Most agencies had weaknesses in access controls, software change controls, segregation of duties, continuity of operations, and agencywide security programs, as shown in table 1. As a result, federal information, systems, and operations were at risk of fraud, misuse, and disruption.

**Table 1: Agencies' Information Security Weaknesses for Fiscal Year 2004**

| Agency/ department | Access controls | Software change controls | Segregation of duties | Continuity of operations | Agencywide security programs |
|---|---|---|---|---|---|
| Agriculture | ■ | ■ | | ■ | ■ |
| AID | ■ | ■ | | | ■ |
| Commerce | ■ | ■ | ■ | ■ | ■ |
| Defense | ■ | ■ | ■ | ■ | ■ |
| Education | ■ | ■ | | | ■ |
| Energy | ■ | ■ | ■ | ■ | ■ |
| EPA | ■ | ■ | ■ | ■ | ■ |
| Homeland Security | ■ | ■ | ■ | ■ | ■ |
| GSA | ■ | ■ | ■ | ■ | ■ |
| HHS | ■ | ■ | | ■ | ■ |
| HUD | ■ | ■ | | ■ | ■ |
| Interior | ■ | ■ | ■ | ■ | ■ |
| Justice | ■ | ■ | ■ | ■ | ■ |
| Labor | ■ | ■ | ■ | ■ | ■ |
| NASA | ■ | ■ | ■ | ■ | ■ |
| NRC | | ■ | | | ■ |
| NSF | ■ | | | ■ | ■ |
| OPM | ■ | ■ | | ■ | ■ |
| SBA | ■ | ■ | ■ | ■ | ■ |
| SSA | ■ | ■ | ■ | ■ | ■ |
| State | ■ | | | | ■ |
| Transportation | ■ | ■ | ■ | ■ | ■ |
| Treasury | ■ | ■ | | ■ | ■ |
| Veterans Affairs | ■ | ■ | ■ | ■ | ■ |

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

Note: Shaded areas indicate weaknesses.

The significance of these weaknesses has led us to continue to report information security as a material weakness[4] in our audit of the fiscal year 2004 financial statements of the U.S. government[5] and to continue to include it in our high risk list.[6] In the 24 major agencies' fiscal year 2004 reporting regarding their financial systems, 10 reported information security as a material weakness and 12 reported it as a reportable condition.[7] Our audits also identified similar weaknesses in nonfinancial systems. In our prior reports, listed in the Related GAO Products section, we have made specific recommendations to the agencies to mitigate identified information security weaknesses. The IGs have also made specific recommendations as part of their information security review work.

## Access Controls Were Not Effectively Implemented

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. As detailed in our methodology for performing information security audits, organizations accomplish this by designing and implementing controls that are intended to prevent, limit, and detect access to computing resources (computers, networks, programs, and data), thereby protecting these resources from unauthorized use, modification, loss, and disclosure. Access controls can be both electronic and physical. Electronic access controls include control of user accounts, use of passwords, and assignment of user rights. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which they are housed. Physical control measures may include guards, badges, and locks, used alone or in combination.

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

[5]Department of the Treasury, *2004 Financial Report of the United States Government*, (Washington, D.C.).

[6]GAO, *High Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

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

Our analysis of IG, agency, and GAO reports has shown that agencies have not always effectively implemented controls to allow only authorized individuals to read, alter, or delete data. Twenty-three of 24 major agencies had access control weaknesses. We identified weaknesses in controls such as user accounts, passwords, and access rights. For example, users created passwords that were common words. Using such words as passwords increases the possibility that an attacker could guess the password and gain access to the account. Also, agencies did not always deactivate unused accounts to prevent them from being exploited by malicious users. In addition, agencies have weaknesses in the controls that prevent unauthorized access to their networks. For example, at one agency, we found an excessive number of connections to the Internet. Each such connection could provide a path for an attacker into the agency's network. Agencies often lacked effective physical barriers to access, including locked doors, visitor screening, and effective use of access cards. Inadequate access controls diminish the reliability of computerized data and increase the risk of unauthorized disclosure, modification, and use. As a result, critical information held by the federal government is at heightened risk of access by unauthorized persons—individuals who could obtain personal data (such as taxpayer information) to perpetrate identity theft and commit financial crimes.

## Software Change Controls Were Not Always in Place

Software change 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. Failure to implement these controls increases the risk that unauthorized programs or changes could be, inadvertently or deliberately, placed into operation.

Our analysis revealed that 22 of the major agencies had weaknesses in software change controls. Weaknesses in this area included the failure to ensure that software was updated correctly and that changes to computer systems were properly approved. In addition, approval, testing, and implementation documentation for changes were not always properly maintained. Consequently, there is an increased risk that programming errors or deliberate execution of unauthorized programs could compromise security controls, corrupt data, or disrupt computer operations.

## Segregation of Duties Was Not Consistently Implemented

Segregation of duties refers to the policies, procedures, and organizational structure that helps ensure that one individual cannot independently control all key aspects of a process or computer-related operation and, thereby, conduct unauthorized actions or gain unauthorized access to assets or records. Proper segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. Dividing duties among individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Without adequate segregation of duties, there is an increased risk that erroneous or fraudulent transactions can be processed, improper program changes implemented, and computer resources damaged or destroyed.

Fourteen agencies had weaknesses regarding segregation of information technology duties. Agencies did not always segregate duties for system administration from duties relating to security administration. For example, individuals at certain agencies could add fictitious users to a system with elevated access privileges and perform unauthorized activities without detection. As a result, these agencies may be exposed to an increased risk of fraud and loss.

## Continuity of Operations Planning Was Often Inadequate

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

Most agencies did not have adequate continuity of operations planning. Twenty of the 24 major agencies had weaknesses in this area. In our April 2005 report on federal continuity of operations plans,[8] we determined that agencies had not developed plans that addressed all the necessary elements. For example, fewer than half the plans reviewed contained adequate contact information for emergency communications. Few plans documented the location of all vital records for the agencies, or methods of updating those records in an emergency. Further, most of the agencies had not conducted tests, training, or exercises frequently enough to have assurance that the plan would work in an emergency. Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission.

## Security Programs Were Not Fully Implemented at Agencies

The underlying cause for the information security weaknesses identified at federal agencies is that they have not yet fully implemented agencywide information security programs. An agencywide security program provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. 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 and disproportionately high expenditures for controls over low-risk resources.

Our analysis has shown that none of the 24 major agencies had fully implemented agencywide information security programs. Agencies often did not adequately assess risks, develop sufficient risk-based policies or procedures for information security, ensure that existing policies and procedures were implemented effectively, or monitor operations to ensure compliance and determine the effectiveness of existing controls. For example, our report on wireless networking[9] at federal agencies revealed that the majority of agencies had not yet identified and responded to the security implications of this emerging technology at their facilities. Agencies had not developed policies and procedures for wireless

[8]GAO, *Continuity of Operations: Agency Plans Have Improved, but Better Oversight Could Assist Agencies in Preparing for Emergencies*, GAO-05-577 (Washington, D.C.: Apr. 28, 2005).

[9]GAO, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*, GAO-05-383 (Washington, D.C.: May 17, 2005).

technology, including configuration requirements, monitoring and compliance controls, or training requirements.

Agencies are also not applying information security program requirements to emerging threats, such as spam, phishing, and spyware,[10] which pose security risks to federal information systems.[11] Spam consumes significant resources and is used as a delivery mechanism for other types of cyber attacks; phishing can lead to identity theft, loss of sensitive information, and use of electronic government services; and spyware can capture and release sensitive data, make unauthorized changes to software, and decrease system performance. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools.

Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded against unauthorized use, disclosure, and modification. Many of the weaknesses discussed have been pervasive for years; our reports attribute them to ineffective security program management—a void that FISMA was enacted to address.

## Government Makes Progress in Implementing FISMA, but Challenges Remain

FISMA provides a comprehensive framework for developing effective agencywide information security programs. Its provisions create a cycle of risk management activities necessary for effective security program management and include requirements for agencies, IGs, NIST, and OMB. The government is progressing in its implementation of the information security management requirements of FISMA, but challenges remain. For example, although the agencies report progress in implementing the provisions of the act, many agencies do not have complete, accurate inventories as required. While the IGs have conducted annual evaluations of the agencies' information security programs as required, the lack of a commonly accepted framework for their evaluations has created issues with consistency and comparability. NIST, however, has developed a

[10]Spam is unsolicited commercial e-mail. Phishing is the practice of using fraudulent messages to obtain personal or sensitive data. Spyware is software that monitors user activity without user knowledge or consent.

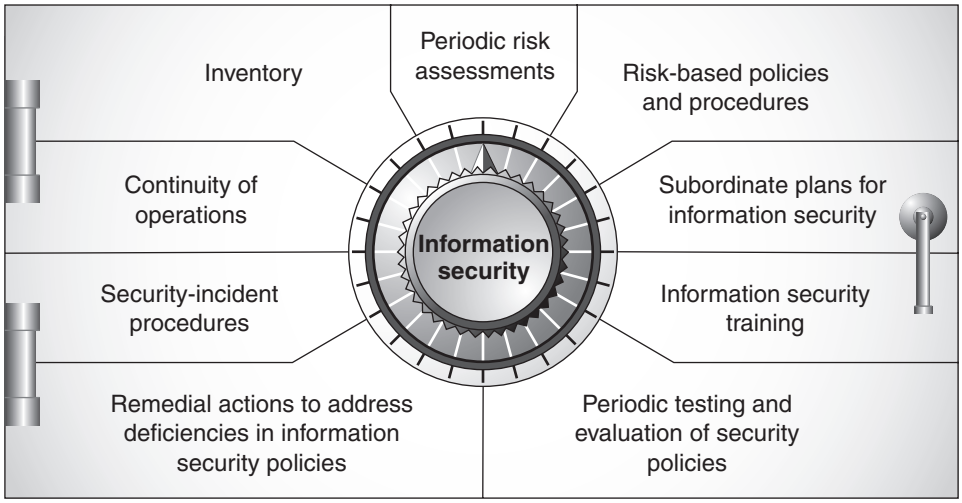
[11]GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 13, 2005).

schedule for its required activities and has begun to issue required guidance, and OMB has issued guidance on the roles and responsibilities of both the agencies and NIST and has also issued annual reporting guidance and reported annually, as required, to the Congress. Our analysis of the annual reporting guidance identified opportunities to increase the usefulness of the reports for oversight.

## Agencies Reporting Progress in FISMA Implementation, but Challenges Remain

FISMA details requirements for the agencies to fulfill in order to develop a strong agencywide information security program. These key requirements are shown in figure 2. A detailed discussion of each of the requirements follows.

**Figure 2: FISMA Requirements for Agency Information Security Programs**




Source: GAO analysis of FISMA.

### Periodic Risk Assessments

As part of the agencywide information security program required for each agency, FISMA mandates that agencies assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of their information and information systems. Risk assessment is the first process in the risk management process, and organizations use risk assessment to determine the extent of the potential threat to information and information systems and the risk associated with an information technology system throughout

its systems development life cycle. Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls.

The Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operations, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and are used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability. Once determined, security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. For fiscal year 2003 FISMA reporting, OMB required agencies to provide the number and percentage of systems assessed for risk.

In fiscal year 2003, half of the 24 major agencies reported assessing the level of risk for 90 to 100 percent of their systems. In addition, our review[12] of 4 agencies' processes for authorizing their systems found that only 72 percent of the 32 systems we reviewed had current risk assessments. Furthermore, we identified one large federal agency that did not have risk assessments for many of its systems. In fiscal year 2004, agencies were not required by OMB to report on the percentage of systems with risk assessments in their FISMA reports; therefore, information on agencies' performance in this area since 2003 is not readily available.

## Risk-Based Policies and Procedures

FISMA requires agencies to include 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 in their information security programs. These policies include determining security control costs and developing minimally acceptable system configuration requirements.

To indicate implementation of the security cost-benefit provisions in FISMA, OMB requires that agencies' budget submissions specifically identify and integrate security costs as part of life-cycle costs for their

[12]GAO, *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operations*, GAO-04-376 (Washington, D.C.: June 28, 2004).

information technology investments. It has also provided criteria to be considered in determining such costs and requires that the agencies report the number of their systems that have security control costs integrated into their system life cycles.

Fiscal year 2004 data for this measure showed that agencies are reporting increases in integrating the cost of security controls into the life cycle of their systems. Specifically, 19 agencies reported integrating security control costs for 90 percent or more of their systems. This represents an increase from 9 agencies in 2003. Governmentwide, OMB reported that 85 percent of agencies' systems had security costs built into the life cycle of the system, an increase of 8 percent from fiscal year 2003. If agencies do not plan for security costs in the life cycle of their systems, they may not allocate adequate resources to ensure ongoing security for federal information and information systems.

FISMA requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In fiscal year 2004, for the first time, agencies reported on the degree to which they had implemented security configurations for specific operating systems and software applications.

Our analysis of the 2004 agency FISMA reports found that 20 agencies reported that they had implemented agencywide policies containing detailed, specific system configurations. However, these agencies did not necessarily have minimally acceptable system configuration requirements for operating systems and software applications that they were running. Specifically, some agencies reported having system configurations, but they did not always implement them on their systems. Of the remaining 4 agencies, 1 reported that it did not have system configurations, and 3 agencies provided insufficient data to determine their status for this measure.

## Subordinate Plans for Information Security

FISMA requires that agencywide information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. These plans are commonly referred to as system security plans. According to NIST guidance, the purpose of these plans is to (1) provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements

and (2) delineate the responsibilities and expected behavior of all individuals who access the system.[13]

In fiscal year 2003, federal agencies reported that they had developed system security plans for 73 percent of agency systems. Although OMB did not require agencies to report on this measure for fiscal year 2004, analysis of the IG FISMA reports for that year revealed that agencies had weaknesses in their system security plans. For example, IGs noted instances where security plans were not developed for all systems or applications. Other weaknesses included plans that were not updated after the systems were significantly modified. Without current, complete system security plans, agencies cannot be assured that vulnerabilities have been mitigated to acceptable levels.

## Information Security Training

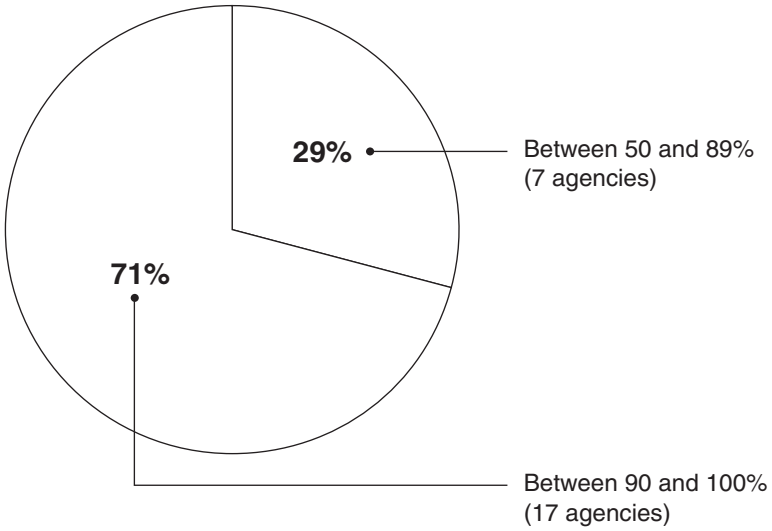
FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide appropriate training on information security to personnel with significant security responsibilities. Agencies reported the number and percentage of employees and contractors who received information security awareness training and the number and percentage of employees with significant security responsibilities who received specialized training.

Our analysis found that agencies were reporting increases in the number and percentages of employees and contractors who have received security awareness training, but many of the agencies reported a decline in the percentage of employees with significant security responsibilities who have received specialized training. For example, 18 of the 24 major agencies reported increasing percentages of employees and contractors who received security awareness training in fiscal year 2004. Furthermore, all 24 agencies reported that they provided security awareness training to 60 percent or more of their employees and contractors for fiscal year 2004, up from 19 agencies in fiscal year 2003. Similarly, 17 agencies reported that

[13]National Institute of Standards and Technology, *Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems*, (Washington, D.C.: December 1998).

they provided security awareness training for 90 percent or more of their employees, an increase from 13 agencies in 2003 (see fig. 3).

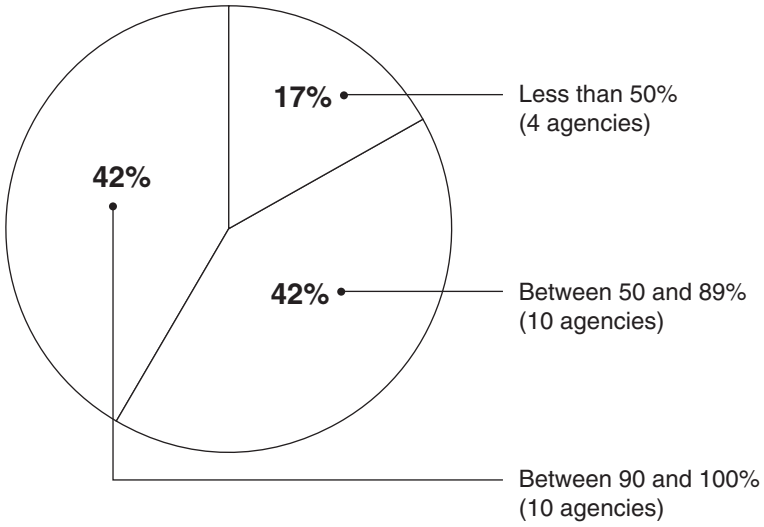
**Figure 3: Percentage of Employees and Contractors Who Received Information Security Awareness Training in Fiscal Year 2004**




Source: GAO analysis of agency-reported data.

However, the governmentwide percentage of employees with significant security responsibilities receiving specialized training decreased from 85 to 81 percent in fiscal year 2004. More specifically, 10 agencies reported decreases in this performance measure. Figure 4 shows the fiscal year 2004 results for this area.

**Figure 4: Percentage of Employees with Significant Security Responsibilities Who Received Specialized Security Training in Fiscal Year 2004**




Source: GAO analysis of agency-reported data.

Failure to provide up-to-date information security awareness training could contribute to the information security problems at agencies. For example, in our report on wireless networks, we determined that the majority of agencies did not address wireless security issues in security awareness training. As a result, their employees may not have been aware of the security risks when they set up unauthorized wireless networks.

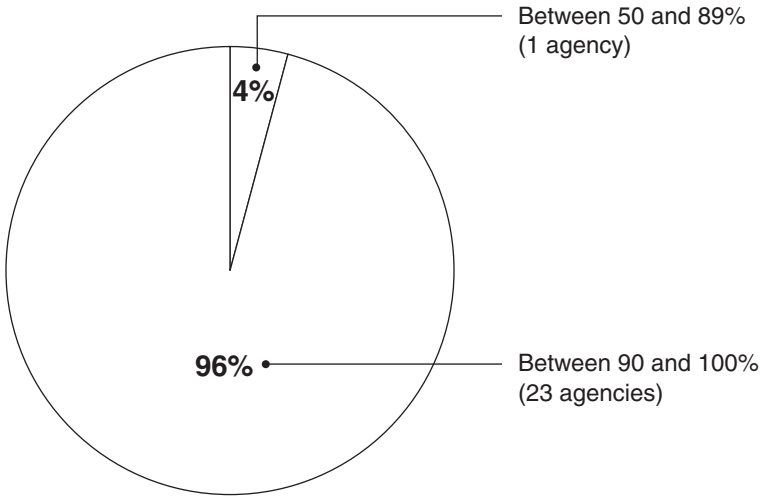
## Periodic Testing and Evaluation of Information Security Policies, Procedures, and Practices

FISMA requires that agency information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency that depends on risk, but no less than annually. This is to include testing of management, operational, and technical controls of every information system identified in the FISMA-required inventory of major systems. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks proactively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of program reviews is an additional source of information that can be considered along with

control testing and evaluation in IG and other independent audits to help provide a more complete picture of the agencies' security postures. OMB requires that agencies report the number of systems annually for which security controls have been reviewed.

In 2004, 23 agencies reported that they had reviewed 90 percent or more of their systems, as compared to only 11 agencies in 2003 that were able to report those numbers (see fig. 5).

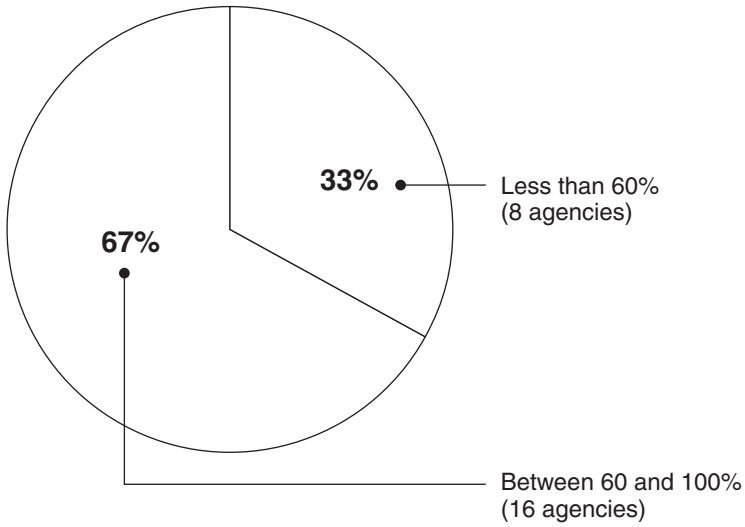
**Figure 5: Percentage of Agency Systems Reviewed during Fiscal Year 2004**




Source: GAO analysis of agency-reported data.

However, agencies have not reported the same progress in addressing reviews of contractor operations. Even though the overall average of contractor operations reviewed for the 24 major agencies increased slightly to 83 percent in fiscal year 2004, 8 agencies reported reviewing less than 60 percent of their contractor operations (see fig. 6). As a result, agencies cannot be assured that federal information and information systems managed by contractors are protected in accordance with agency policies.

**Figure 6: Percentage of Contractor Operations Reviewed during Fiscal Year 2004**




Source: GAO analysis of agency-reported data.

Our recent report on the oversight of contractor operations[14] indicated that the methods that agencies are using to ensure information security oversight have limitations and need strengthening. For example, most agencies have not incorporated FISMA requirements, such as annual testing of controls, into their contract language. Additionally, most of the 24 major agencies reported having policies for contractors and users with privileged access to federal data and systems; however, our analysis of submitted agency policies found that only 5 agencies had established specific information security oversight policies. Finally, while the majority of agencies reported using a NIST self-assessment tool to review contractor security capabilities, only 10 agencies reported using the tool to assess users with privileged access to federal data and systems, which may expose federal data to increased risk.

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

Another requirement of FISMA is that agencies' information security programs include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in information security policies, procedures, and practices. Developing effective

[14]GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, GAO-05-362 (Washington, D.C.: April 22, 2005).

corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. These remediation plans, called plans of action and milestones by OMB, are to list the weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions. OMB requires agencies to report whether they have a remediation plan for all programs and systems where a security weakness has been identified. OMB also requested that IGs assess whether the agency has developed, implemented, and managed an agencywide process for these plans.

According to the IGs' assessments of their agencies' remediation processes, 14 of the 24 major agencies did not almost always incorporate information security weaknesses for all systems into their remediation plans. The IGs also reported that 13 agencies did not use the remediation process to prioritize information security weaknesses more than 95 percent of the time to help ensure that significant weaknesses are addressed in an efficient and timely manner. Without a sound remediation process, agencies cannot efficiently and effectively correct weaknesses in their information security programs.

## Security Incident Procedures

Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. Problem and incident reports can, therefore, provide valuable input for risk assessments, help in prioritizing security improvement, and be used to illustrate risks and related trends in reports to senior management.

FISMA requires that agencies' information security programs include procedures for detecting, reporting, and responding to security incidents; mitigating risks associated with such incidents before substantial damage is done; and notifying and consulting with the information security incident center and other entities, as appropriate, including law enforcement agencies and relevant IGs. NIST has provided guidance to assist organizations in establishing computer security incident-response capabilities and in handling incidents efficiently and effectively. OMB requires agencies to report information related to security incident reporting. This information includes whether the agency follows

documented policies and procedures for reporting incidents internally, externally to law enforcement, and to the United States Computer Emergency Readiness Team (US-CERT).[15]

Information reported for this requirement varied widely across the agencies. Some agencies reported relatively few incidents internally (fewer than 10), while others reported as many as 600,000 incidents. Half (12 of 24) of the major agencies' CIOs stated that they reported between 90 and 100 percent of incidents to US-CERT. One agency reported between 75 and 89 percent of incidents to US-CERT. The other agencies said that they reported 49 percent or fewer of their incidents to US-CERT or provided information that was not comparable. OMB stated in its March 1, 2005, FISMA report that it was concerned that very low numbers of incidents were being reported to US-CERT. Our work in this area[16] also indicated that agencies were not consistently reporting security incidents. Without adequate reporting, the federal government cannot be fully aware of possible threats.

## Continuity of Operations

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. Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, accidental loss of files, or a major disaster. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations.

The testing of contingency plans is essential to determining whether the plans will function as intended in an emergency situation. The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data

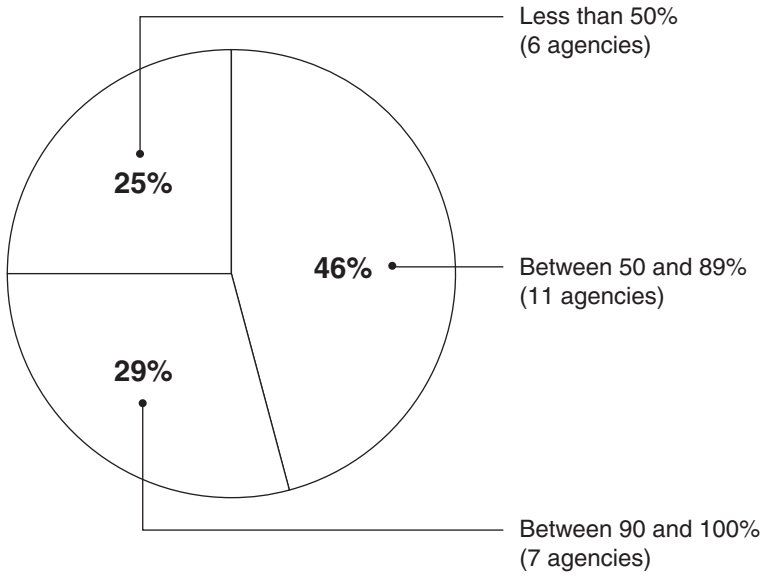
[15]FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by DHS's US-CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination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

[16]GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 13, 2005).

processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. To show the status of implementing this requirement, OMB required that agencies report the percentage of systems that have a contingency plan and the percentage that have contingency plans that have been tested.

Overall, federal agencies reported that 57 percent of their systems had contingency plans that had been tested. Although 19 agencies reported increases in the testing of contingency plans, 6 agencies reported that less than 50 percent of their systems had tested contingency plans (see fig. 7).

**Figure 7: Percentage of Systems with Contingency Plans that Have Been Tested for Fiscal Year 2004**




Source: GAO analysis of agency-reported data.

Also, three agencies reported having contingency plans for all their systems and only 1 reported testing the plans for all their systems. Without testing, agencies have limited assurance that they will be able to recover mission-

critical applications, business processes, and information in the event of an unexpected interruption.

### Inventory of Major Systems

FISMA also requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. A complete and accurate inventory of major information systems is a key element of managing the agency's information technology resources, including the security of those resources. The inventory is used to track the agency systems for annual testing and evaluation and contingency planning. In addition, the total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affect the percentage of systems shown as meeting the requirements.

In fiscal year 2004 FISMA reports, 20 of the 24 major agencies reported having complete, accurate inventories that were updated at least annually. There was disagreement among the agencies and IGs regarding the accuracy of the number of programs, systems, and contractor operations or facilities. For instance, although 20 agencies reported having inventories that were updated at least annually, only 8 IGs agreed with the accuracy of those inventories. Without complete, accurate inventories, agencies cannot efficiently maintain and secure their systems. Moreover, the performance measures that are stated as a percentage of systems, including systems and contractor operations reviewed annually, continuity plans tested, and certification and accreditation, may not accurately reflect the extent to which these security practices have been implemented.

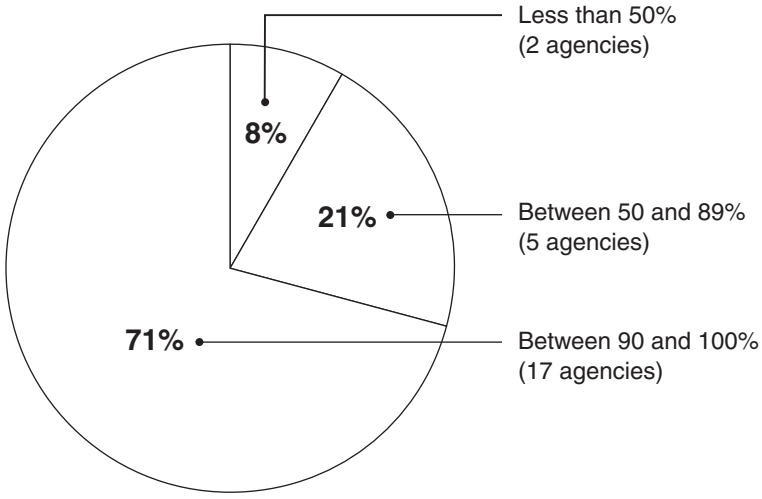
### Certification and Accreditation

In addition to the FISMA requirements, OMB requires agencies to report on their certification and accreditation process. Certification and accreditation is the requirement that agency management officials formally authorize their information systems to process information; thereby accepting the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. This process is not included in FISMA but does include statutory requirements such as risk assessments and security plans. Therefore, OMB eliminated separate reporting requirements for risk assessments and security plans. For annual reporting, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation.

For fiscal year 2004, OMB's guidance also requested that IGs assess their agencies' certification and accreditation process.

Data reported for this measure showed overall increases for most agencies. According to OMB, 77 percent of government systems had undergone certification and accreditation for fiscal year 2004. For example, 19 of the 24 major agencies reported increasing percentages from fiscal year 2003 to fiscal year 2004. In addition, 17 agencies reported percentages of systems certified and accredited at or above 90 percent (see fig. 8).

**Figure 8: Percentage of Systems during Fiscal Year 2004 that Were Authorized for Processing after Certification and Accreditation**




Source: GAO analysis of agency-reported data.

Although agencies have reported progress in certifying and accrediting their systems, weaknesses in the process remain. In a previously issued report,[17] we determined that agencies were unclear on the number of systems that undergo the process, were inconsistent in their reporting of certification and accreditation performance data, and lacked quality assurance policies and procedures relating to the certification and accreditation process.

[17]GAO, *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation*, GAO-04-376 (Washington, D.C.: June 28, 2004).

The IGs also reported weaknesses in the certification and accreditation process in their fiscal year 2004 FISMA reports. For example, IGs reported systems that did not have formal authorization to operate or were missing critical elements such as security plans, risk assessments, and contingency plans. Furthermore, OMB's March 2005 report to Congress noted that seven IGs rated their agencies' certification and accreditation process as poor. Therefore, agencies' reported data may not accurately reflect the status of an agency's implementation of this requirement.

## Inspectors General Fulfill FISMA Requirements but Lack Framework

FISMA requires the IGs to perform an independent evaluation of the information security program and practices of the agency to determine the effectiveness of such programs and practices. Each evaluation should 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.

The IGs have conducted annual evaluations as required and have reported on the results. However, they do not have a common approach to the annual evaluations. As a result, IGs may not be performing their evaluations with peak effectiveness, efficiency, and adequate quality control.

A commonly accepted framework or methodology for the FISMA independent evaluations could provide improved effectiveness, increased efficiency, quality control, and consistency of application. Such a framework may provide improved effectiveness of the annual evaluations by ensuring that compliance with FISMA and all related guidance, laws, and regulations is considered in the performance of the evaluation. IGs may be able to use the framework to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently. A commonly accepted framework may offer quality control by providing a standardized methodology that can be followed by all personnel. Finally, IGs may obtain consistency of application through a documented methodology.

A commonly accepted framework for performing the annual FISMA evaluation could offer additional benefits as well. For example, it might allow the IGs to coordinate on information security issues, weaknesses, and initiatives that cross agency lines. It could also facilitate appropriate

coverage of major federal contractors who serve multiple federal agencies. Such a framework could provide assistance to the smaller IG offices by allowing them to leverage lessons learned by larger IG offices, for example, through the development and use of model statements of work for FISMA contracts.

Finally, the usefulness and comparability of the IGs' annual evaluations for oversight bodies may be improved by the adoption of a framework for the FISMA independent evaluations. The current inconsistencies in methodology affect the consistency and comparability of reported results. As a result, the usefulness of the IG reviews for assessing the governmentwide information security posture is potentially reduced.

The President's Council on Integrity and Efficiency[18] has recognized the importance of having a framework and is working to develop one for FISMA reviews. The Council is including both OMB and us in its deliberations. The Council, which currently maintains *The Financial Audit Manual*, a commonly accepted framework for the performance of government financial audits, brings expertise and experience to the development of a FISMA evaluation framework.

## NIST Maintains Timely Release of Guidance

NIST has developed a plan for releasing important guidance for the agencies and fulfilling its other responsibilities under FISMA. NIST is required, among other things, to issue guidance on information security policies and practices for the agencies, provide technical assistance, conduct research as needed in information security, and assist in the development of standards for national security systems.

After FISMA was enacted, NIST developed the FISMA Implementation Project to enable it to fulfill its statutory requirements in a timely manner. The project is divided into three phases. Phase I focuses on the development of a suite of security standards and guidelines required by FISMA as well as other FISMA-related publications necessary to create a robust information security program and effectively manage risk to agency operations and agency assets. NIST has already issued one FIPS, which

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

covers the categorization of systems according to risk. A second FIPS concerning the minimum security requirements for each risk category is due out soon. NIST has also issued guidance to assist the agencies in determining the correct risk level for systems and mapping the systems to the correct categories. This stage is due to be completed in 2006. The status of the guidance is shown in figure 9.

**Figure 9: Status of FISMA Guidance at NIST**

| FISMA implementation project publications | | Mar 05 | Apr 05 | May 05 | June 05 | July 05 | Aug 05 | Sept 05 | Oct 05 | Nov 05 | Dec 05 | Jan 06 | Feb 06 | Mar 06 | Apr 06 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FIPS 199 | Final | | | | | | | | | | | | | | |
| FIPS 200 | | | | | IPD | PCP | RVC | RVC | RVC | RVC | Final | | | | |
| SP-800-37 | Final | | | | | | | | | | | | | | |
| SP-800-53 | Final | | | | | | | | | | | | | | |
| SP-800-53A | | | | | IPD | PCP | RVC | RVC | RVC | SPD | PCP | RVC | RVC | FPD | Final |
| SP-800-59 | Final | | | | | | | | | | | | | | |
| SP-800-60 | Final | | | | | | | | | | | | | | |
| Related publications | | | | | | | | | | | | | | | |
| SP-800-26 | | | | | IPD | PCP | RVC | RVC | RVC | Final | | | | | |
| SP-800-18 | | | | | IPD | PCP | RVC | Final | | | | | | | |

IPD Initial public draft
SPD Second public draft
FPD Final public draft
PCP Public comment draft
RVC Revision cycle
Final Completed

Source: NIST.

Notes:

FIPS 199: Standards for Security Catagorization of Federal Information and Information Systems

FIPS 200: Minimum Security Requirements for Federal Information Systems

SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems

SP 800-53: Recommended Security Controls for Federal Information Systems

SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems

SP 800-59: Guideline for Identifying an Information System as a National Security System

SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

SP 800-26: Assessment Guide for Information Systems and Security Programs

SP 800-18: Guide for Developing Security Plans for Federal Information Systems

Phase II will focus on the development of a program for accrediting public and private sector organizations to conduct security certification services for federal agencies, as part of agencies' certification and accreditation requirements. Organizations that participate in the organizational accreditation program[19] can demonstrate competency in the application of NIST security standards and guidelines. NIST states that developing a network of accredited organizations with demonstrated competence in the provision of security certification services will give federal agencies greater confidence in the acquisition and use of such services. Phase II is planned for fiscal year 2006.

Phase III is the development of a program for validating security tools. The program will rely on private sector, accredited testing laboratories to conduct evaluations of the security tools. NIST will provide validation services and laboratory oversight. Implementation of this phase is also planned for fiscal year 2006.

The agency has also made progress in implementing other requirements. For example, it is continuing to provide consultative services to agencies on FISMA-related information security issues and has established a Web site for federal agencies to identify, evaluate, and disseminate best practices for critical infrastructure protection and security. In addition, it has established a Web site for the private sector to share nonfederal information security practices. NIST has continued an ongoing dialogue with the National Security Agency and the Committee on National Security Systems to coordinate and take advantage of the security work these entities have under way within the federal government.

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

- operating a computer security expert assist team to assist federal agencies in identifying and resolving security problems;

- conducting security research in areas such as access control, wireless, mobile agents, smart cards, and quantum computing;

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

- improving the security of control systems that manage key elements of the country's critical infrastructure; and

- performing cyber security product certifications required for government procurements.

Finally, NIST issued its annual status reports as required by FISMA in April of 2003 and 2004.

## OMB Oversees FISMA Implementation, but Analysis of Annual Reporting Guidance Identified Opportunities for Improvement

According to FISMA, the Director of OMB is responsible for developing and overseeing the implementation of information security at the agencies. OMB reported that it has used the information gathered under this act to assist it in focusing its attention and resources on poorly performing agencies.

To oversee the implementation of policies and practices relating to information security, OMB has issued guidance to the agencies on their requirements under FISMA. In its annual memorandum on reporting, it instructed agencies that the use of NIST standards and guidance was required. OMB has updated its budget guidance[20] to gather data on information security at the agencies. For example, it asks the agencies to estimate a percentage of the total investment in information technology that is associated with security. Agencies are asked to consider the products, procedures, and personnel that are dedicated primarily to provision of security. These procedures include FISMA requirements, such as risk assessments, security plans, education and training, system reviews, remedial plans, contingency planning and testing, and reviews or inspections of contractor operations.

To oversee agency compliance with FISMA, OMB relies on annual reporting by the agencies and the IGs. It reported the results of this annual reporting to Congress by March 1 in 2004 and 2005, as required by FISMA. In these reports, it evaluated the agencies' reported data against performance measures it had developed. On August 23, 2004, OMB issued its fiscal year 2004 reporting instructions. The reporting instructions, similar to the 2003 instructions, emphasized a strong focus on performance measures and

[20]Office of Management and Budget, *Circular A-11: Preparation, Submission and Execution of the Budget* (Washington, D.C.: July 2004).

formatted these instructions to emphasize a quantitative, rather than a narrative, response.

OMB stated that it is using a combination of sources to fulfill its requirement under FISMA to annually approve or disapprove of agencies' information security programs; some information is taken from security and privacy information submitted by the agencies during the budget process, and other information comes from the annual reporting.

## Analysis of Annual Reporting Identifies Opportunities to Enhance Oversight of Agency Implementation

Periodic reporting of performance measures for FISMA requirements and related analysis provides valuable information on the status and progress of agency efforts to implement effective security management programs. However, as we have recently testified,[21] our analysis of OMB's annual reporting guidance identified areas where additional reporting requirements would increase usefulness of annual reports for oversight. These areas include reporting on the quality of agency processes, risk-based reporting of data, including key FISMA requirements, and ensuring clarity.

### Limited Assurance of the Quality of Agency Processes

Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, for the annual review process, agencies report the number of agency systems and contractor operations they reviewed. They also report on, and the IGs confirm, whether they used appropriate guidance. However, reporting on the quality of the reviews, such as whether guidance was applied correctly or if results were tracked for remediation, is not required. Moreover, as mentioned previously, our work in this area revealed that the methods agencies were using for the reviews had limitations and needed strengthening. Providing information on the quality of the review process would further enhance the usefulness of the annually reported data in this area for management and oversight purposes.

OMB has recognized the need for assurance of quality for agency processes. For example, it specifically requested that the IGs evaluate the plan of action and milestones process and the certification and

[21]GAO, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, GAO-05-483T (Washington, D.C.: Apr. 7, 2005).

accreditation process at their agencies. The results of these evaluations call into question the reliability and quality of the data reported by several agencies. Therefore, increased risk exists that the performance data reported by the agencies may not accurately reflect the status of agencies' implementation of these information security activities.

**Data Not Reported According to System Risk**

Performance measurement data are reported on the total number of agency systems but do not indicate the assessed level of risk of those systems. Reporting by system risk could provide information about whether agencies are prioritizing their information security efforts according to risk. For example, the performance measures for fiscal year 2004 show that 57 percent of the total number of systems have tested contingency plans, but do not indicate to what extent this 57 percent includes the agencies' high or moderate risk systems. Therefore, agencies, the administration, and Congress cannot be sure that critical federal operations can be restored if an unexpected event disrupts service.

**Reporting Does Not Include Aspects of Key Requirements**

Currently, OMB reporting guidance and performance measures do not include separate and complete reporting on FISMA requirements. For example, FISMA requires agencies to have procedures for detecting, reporting, and responding to security incidents. Currently, the annual reporting developed by OMB focuses on incident reporting: how the agencies are reporting their incidents internally to law enforcement and to the US-CERT. Although incident reporting is an important aspect of incident handling, it is only one part of the process. Additional questions that cover incident detection and response activities would be useful to oversight bodies in determining the extent to which agencies have implemented capabilities for managing security incidents.

Reporting on the remediation process does not include a key aspect of this process. Current reporting guidance asks about the inclusiveness of the plans, i.e. whether all known information security weaknesses are included; however, if and how weaknesses are mitigated is not reported. For example, the agencies do not report what percentage of existing weaknesses they have remedied during the year. In addition, agencies do not report the risk level of the systems on which the weaknesses are found. Valuable information may be provided to oversight bodies by posing additional questions on the remediation process.

The annual reporting process also does not include separate reporting on certain FISMA requirements. For example, in the 2004 guidance, OMB eliminated separate reporting on risk assessments and security plans. Because the guidance on the certification and accreditation process required both risk assessments and security plans, OMB did not require agencies to answer separate questions in these areas. Although OMB did ask for the IGs' assessments of the certification and accreditation process, it did not require them to comment separately on these specific requirements. As a result, agency management, Congress, and OMB do not have complete information on the status of agencies' implementation efforts for these requirements.

**Reporting Instructions Need Clarity**

Several questions in OMB's 2004 reporting guidance could be subject to differing interpretations by IGs and the agencies. For example, one of the questions asked the IGs whether they and their agency used the plan of actions and milestones as a definitive management tool; however, IGs are not required to use these plans. Therefore, a negative answer to this question could mean either that the agency and the IG were not using the plan, or that one of them was not using the plan. As a result, it may erroneously appear that agencies were not using the plans as the major management tool for remediation of identified weaknesses as required by OMB.

Another example of differing interpretations was one of the inventory questions. It asked if the IG and agency agreed on the number of programs, systems, and contractor operations in the inventory. Since the question could be interpreted two ways, the meaning of the response was unclear. For example, if an IG replied in the negative, it could mean that while the IG agreed with the total numbers in the inventory, it disagreed with how the agency identified whether the inventory entry was a program, system, or contractor operations. Alternatively, a negative response could mean that the IG disagreed with the overall accuracy of the inventory. Additional questions in the areas of configuration management and certification and accreditation also generated confusion. As a result, unclear reporting instructions may have decreased the reliability and consistency of reported performance data.

## Conclusions

Federal agencies have not consistently implemented effective information security policies and practices. As a result, pervasive weaknesses exist in

almost all areas of information security controls. These weaknesses place federal operations and assets at risk of fraud, misuse, and abuse, and may put financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. In our prior reports, as well as in reports by the IGs, specific recommendations were made to the agencies to mitigate identified information security weaknesses.

The government is progressing in implementing FISMA requirements; the agencies, IGs, NIST, and OMB have all made advances in fulfilling their requirements. However, current reporting under FISMA by the agencies produces performance data that may not accurately reflect the status of agencies' implementation of required information security policies and procedures. Oversight entities are not able to determine from the reports a true or complete picture of the adequacy and effectiveness of agencies' information security programs. However, opportunities exist to improve reporting guidance that might lead to more useful and complete information on the implementation of agencies' information security programs. Until such information is available, there is little assurance that the pervasive weaknesses in agencywide information security programs are being addressed.

## Recommendations for Executive Action

We recommend that the Director of OMB take the following four actions in revising future FISMA reporting guidance:

- request the inspectors general to report on the quality of additional agency processes, such as the annual system reviews;
- require agencies to report FISMA data by risk category;
- ensure that all aspects of key FISMA requirements are reported on in the annual reports; and
- review guidance to ensure clarity of instructions.

## Agency Comments and Our Evaluation

In written comments on a draft of this report (reprinted in app. II), the Administrator, Office of E-Government and Information Technology, OMB, agreed with our overall assessment of information security at the agencies, but disagreed with one of our recommendations to enhance FISMA

reporting guidance and provided comments on the others. In addition, the Administrator made several general comments.

In commenting on our recommendation that OMB guidance request that the IGs report on the quality of additional agency processes, OMB stated that their current guidance has provided the IGs with the opportunity to include supporting narrative responses for all questions and that the guidance encourages the IGs to provide any additional meaningful information they may have. We acknowledge that OMB has given the agency IGs the opportunity to include such additional information as they believe may be helpful. However, since specific information was not requested, the resulting information that was reported, if any, was not consistent or comparable across the agencies and over time. In our report, we noted that OMB has recognized the need for assurance of quality for agency processes. For example, OMB specifically requested that the IGs evaluate the plans of actions and milestones and the certification and accreditation processes at their agencies. We believe that additional processes should be assessed for quality such as the annual system review process. This would further enhance the usefulness of the annually reported data for management and oversight purposes.

Regarding our recommendation to include FISMA data by risk category, OMB noted in its comments that this recommendation is now addressed by its fiscal year 2005 FISMA reporting guidance. This guidance was issued in June 2005.

In responding to our recommendation to ensure that all key FISMA requirements are reported on in the annual reports, OMB disagreed with our assessment that additional sub-elements are necessary in its reporting guidance and stated that its reporting guidance satisfies all FISMA requirements through a combination of data collection and specialized questions. OMB cited as examples its performance data on agencies' certification and accreditation processes and its questions to IGs regarding the quality of agency corrective plans of actions and milestones. In addition, it commented that its guidance complied with the remainder of FISMA's reporting requirements by having agencies respond to specialized questions. As noted in our report, some FISMA requirements are not specifically being addressed through these means, such as reporting on risk assessments, subordinate security plans, security incident detection and response activities, and whether weaknesses are mitigated. We agree with OMB that the process of certification and accreditation requires agencies to document risk assessments and security plans. However, as stated in our

report, the IGs reported the certification and accreditation processes included missing security plans, risk assessments, and contingency plans. Furthermore, seven IGs rated their agencies' certification and accreditation processes as poor. Since the quality of the certification and accreditation processes at some agencies has been called into question by the IGs, we believe reporting separately on the risk assessments and security plans at this time may provide better information on the status of agencies' information security implementation efforts.

OMB commented on our recommendation that it review guidance to ensure clarity of instructions by stating that its staff worked with agencies and the IGs throughout the year when developing the guidance and, in particular, during the reporting period to ensure that agencies adequately understood the reporting instructions. We acknowledge OMB's efforts to help ensure better clarity, but believe more needs to be done. As noted in this report, several questions in the guidance could be subject to differing interpretations. For example, questions in the areas of plans of actions and milestones, inventory, configuration management, and certification and accreditation generated confusion. As a result, the reported data may contain erroneous information, and its reliability and consistency could be decreased.

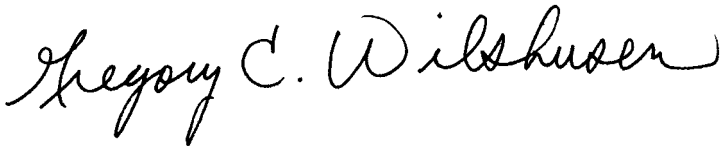
OMB also strongly disagreed with any inference in the draft report that its reporting guidance fails to meet the requirements of FISMA. We did not make such a statement. Rather, our report provides that OMB needs to enhance its reporting guidance to the agencies so that the annual FISMA reports provide more information essential for effective oversight.

Similarly, OMB commented that our report included the suggestion that, unless it asked a specific question in a particular way and agencies answered those questions once each year, agencies would not implement FISMA nor provide adequate cost-effective security for their information and systems. This characterization of our report is incorrect. We noted that specific recommendations were previously made to the agencies to remedy identified information security weaknesses. Our recommendations in this report address the need for OMB to enhance its FISMA reporting guidance to increase the effectiveness and reliability of annual reporting.

Our report also emphasized the need to improve FISMA data for oversight purposes. We believe that OMB can achieve this by implementing our recommendations.

We are sending copies of this report to the Director of OMB and to interested congressional committees. We will also make copies available to others upon request. In addition, the report will be available on GAO's Web site at http://www.gao.gov.

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



Gregory C. Wilshusen
Director, Information Security Issues

# Objectives, Scope, and Methodology

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

To assess the adequacy and effectiveness of agencies' information security policies and practices, we analyzed our related reports issued from the beginning of fiscal year 2003 through May of 2005. We also reviewed and analyzed the information security work and products of the IGs. Both our reports and the IGs' products used the methodology contained in *The Federal Information System Controls Audit Manual*. Further, we reviewed and analyzed data on information security in federal agencies' performance and accountability reports.

To assess implementation of FISMA requirements, we reviewed and analyzed the Federal Information Security Management Act (Public Law 107-347); the 24 major federal agencies' and Office of Inspector General FISMA reports for fiscal years 2003 and 2004, as well as the performance and accountability reports for those agencies; the Office of Management and Budget's FISMA guidance and mandated annual reports to Congress; and the National Institute of Standards and Technology's standards, guidance, and annual reports. We also held discussions with agency officials and the agency inspectors general to further assess the implementation of FISMA requirements. We did not include systems categorized as national security systems in our review, nor did we review the adequacy or effectiveness of the security policies and practices for those systems.

Our work was conducted in Washington, D.C., from September 2004 through May 2005 in accordance with generally accepted government auditing standards.

# Comments from the Office of Management and Budget

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

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

JUN 29 2005

Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, SW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on GAO's draft report on agency implementation of the Federal Information Security Management Act (FISMA), "INFORMATION SECURITY: Weaknesses Persists at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements" (GAO-05-552).

FISMA is the foundation of the Federal government's information security program, and we appreciate GAO's careful analysis of FISMA's requirements. In particular, we value GAO identifying specific persistent information security problems at the agencies, and agree that improvement is needed.

GAO's draft report includes four recommendations for OMB regarding agency reporting on FISMA. In particular, GAO's draft report recommends OMB expand its existing reporting guidance to agencies to include additional elements.

See comment 1.

OMB disagrees however, that additional sub-elements are necessary and strongly disagrees with any inference in the draft report that OMB's reporting guidance fails to meet the requirements of FISMA. OMB's reporting instructions satisfy all FISMA requirements through a combination of data collection and specialized questions. For instance, OMB collects performance data from the agencies (including their Inspectors General (IG) on their certification and accreditation processes. This requires agencies to document all components of security planning such as risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, privacy impact assessments, and system interconnection agreements. Similarly, in asking IGs about the quality of agency corrective plans of action and milestones, an essential element of any security program is specifically addressed. Beyond certification and accreditation and plans of action and milestones, OMB's guidance complies with the remainder of FISMA's reporting requirements by having agencies respond to specialized questions. These questions deal with matters such as documented procedures for securing emerging technologies and how agencies ensure secure contractor operations.

See comment 2.

Additionally, the draft report infers that unless OMB asks a specific question in a particular way and agencies answer those questions once each year, agencies' will not implement FISMA nor provide adequate cost-effective security for their information and systems. Reporting to OMB is only one part of FISMA and the comprehensive agency information security program called for in the Act. Scarce agency resources should focus on developing and

implementing a program to secure information and systems. Even if we agreed OMB's reporting guidance was deficient in some way, the simple fact is responsibility and accountability for implementation and compliance with FISMA rests in the agencies monitoring their own performance throughout the year.

See comment 3.

In addition to expanded reporting elements, the draft report recommends that OMB's guidance include a requirement that agency Inspector Generals (IGs) report on the quality of agency processes, such as the annual system review. OMB's guidance already provides IGs with the opportunity to include supporting narrative responses for all questions and encourages IGs to provide any additional meaningful information they may have. Agency IG narratives are especially significant to OMB's assessment of the certification and accreditation process because it includes many key FISMA elements.

See comment 4.

The draft report also recommends that OMB review our guidance to ensure clarity. OMB staff work with agencies and the IGs throughout the year, when developing the guidance, and in particular during the reporting period, to ensure that agencies adequately understand our reporting instructions.

See comment 5.

Finally, we note that the recommendation to include FISMA data by risk category is addressed by OMB's FY 2005 FISMA reporting guidance. Such reporting would not have been meaningful until the National Institute of Standards and Technology (NIST) issued specific guidance on risk categorization as they did last year. Since the guidance has been issued, we are asking agencies to report by the NIST categories.

See comment 6.

Thank you for the opportunity to review and comment on your draft report on this important issue of information security. While we agree with your assessment that information security in the agencies can and should continue to improve, we do not agree with the solutions you propose in your draft report.

Sincerely,

Karen S. Evans
Administrator
Office of E-Government and
Information Technology

The following are GAO's comments on OMB's letter dated June 29, 2005.

## GAO Comments

1. As noted in our report, some FISMA requirements are not specifically being addressed by OMB's reporting instructions, such as reporting on risk assessments, subordinate security plans, security incident detection and response activities, and whether weaknesses are mitigated. We agree with OMB that the process of certification and accreditation requires agencies to document components of security planning such as risk assessment. However, as stated in our report, the IGs reported the certification and accreditation process included missing security plans, risk assessments, and contingency plans. Furthermore, seven IGs rated their agencies' certification and accreditation processes as poor. Since the quality of the certification and accreditation process has been called into question by some IGs, we believe that reporting separately on the components at this time may provide better information on the status of agencies' information security implementation efforts. Also, we disagree that our report indicates that OMB's reporting guidance fails to meet the requirements of FISMA. We did not make such a statement. Rather, our report provides that OMB needs to enhance its reporting guidance to the agencies so that the annual FISMA reports provide more information essential for effective oversight.

2. We disagree with OMB comments that our report included the suggestion that unless OMB asked a specific question in a particular way and agencies answered those questions once each year, agencies would not implement FISMA nor provide adequate cost-effective security for their information and systems. We make no such statement or suggestion. OMB also stated that responsibility and accountability for implementation and compliance with FISMA rests with the agencies, including monitoring their own performance throughout the year. As noted in our report, FISMA clearly defines separate roles and responsibilities for federal agencies and their IGs, NIST, and OMB, to provide a comprehensive framework for ensuring the effectiveness of information security controls. Therefore, we cannot fully agree with OMB's statement that responsibility and accountability for implementation and compliance with FISMA rests with the agencies. All parties included in the act share in the responsibility. We do agree, however, that FISMA includes the requirement that agencies monitor their own performance throughout the year.

3. OMB's reporting guidance does not specifically address the issue of the quality of agency processes used to gather information for FISMA reporting. We acknowledge that OMB has given the agency IGs the opportunity to include such additional information as they believe may be helpful. However, since specific information has not been requested, the resulting reported information has not been consistent or comparable across the agencies and over time. In our report we noted that OMB has recognized the need for assurance of quality for certain agency processes. For example, it specifically requested that the IGs evaluate the plan of actions and milestones process and the certification and accreditation process at their agencies. We believe that additional processes should be assessed for quality such as the annual system reviews. Providing information on the quality of the review process would further enhance the usefulness of the annually reported data for management and oversight purposes.

4. We acknowledge OMB's efforts to help ensure better clarity but believe more needs to be done. As we noted in our report, several questions could be subject to differing interpretations. Questions in the areas of plans of actions and milestones, inventory, configuration management, and certification and accreditation generated confusion. As a result, the reported data may contain erroneous information, and its reliability and consistency may be decreased.

5. The guidance to report FISMA data by risk category was issued on June 13, 2005—after our draft report was provided to OMB for comment. Reporting by system risk could provide information about whether agencies are appropriately prioritizing their information security efforts.

6. In this report, we do not propose solutions to agency information security weaknesses. Rather, we reported that pervasive weaknesses in federal agencies' information security policies and practices place data at risk. This statement is supported by our prior reports and reports by the IGs. We noted that, in those prior reports, specific recommendations were made to the agencies to remedy identified information security weaknesses. In this report, we recommended that OMB enhance FISMA reporting guidance to increase the effectiveness and reliability of annual reporting.

# GAO Staff Acknowledgments

## Staff Acknowledgments

Larry Crosland, Season Dietrich, Nancy Glover, Carol Langelier, Suzanne Lightman, and Stephanie Lee made key contributions to this report.

# Related GAO Products

*Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress*. GAO-05-486. Washington, D.C.: May 19, 2005.

*Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks*. GAO-05-383. Washington, D.C.: May 17, 2005.

*Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*. GAO-05-231. Washington, D.C.: May 13, 2005.

*Continuity of Operations: Agency Plans Have Improved, but Better Oversight Could Assist Agencies in Preparing for Emergencies.* GAO-05-577. Washington, D.C.: April 28, 2005.

*Continuity of Operations: Agency Plans Have Improved, but Better Oversight Could Assist Agencies in Preparing for Emergencies.* GAO-05-619T. Washington, D.C.: April 28, 2005.

*Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*. GAO-05-362. Washington, D.C.: April 22, 2005.

*Information Security: Internal Revenue Service Needs to Remedy Serious Weaknesses over Taxpayer and Bank Secrecy Act Data*. GAO-05-482. Washington, D.C.: April 15, 2005.

*Information Security: Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements*. GAO-05-567T. Washington, D.C.: April 14, 2005.

*Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*. GAO-05-483T. Washington, D.C.: April 7, 2005.

*Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*. GAO-05-262. Washington, D.C.: March 23, 2005.

*High-Risk Series: An Update.* GAO-05-207. Washington, D.C.: January 2005.

*Financial Management: Department of Homeland Security Faces Significant Financial Management Challenges*. GAO-04-774. Washington, D.C.: July 19, 2004.

*Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation*. GAO-04-376. Washington, D.C.: June 28, 2004.

*Information Technology: Training Can Be Enhanced by Greater Use of Leading Practices*. GAO-04-791. Washington, D.C.: June 24, 2004.

*Information Security: Agencies Face Challenges in Implementing Effective Software Patch Management Processes*. GAO-04-816T. Washington, D.C.: June 2, 2004.

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

*Information Security: Information System Controls at the Federal Deposit Insurance Corporation*. GAO-04-630. Washington, D.C.: May 28, 2004.

*Technology Assessment: Cybersecurity for Critical Infrastructure Protection*. GAO-04-321. Washington, D.C.: May 18, 2004.

*Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Services*. GAO-04-638T. Washington, D.C.: April 22, 2004.

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. GAO-04-628T. Washington, D.C.: March 30, 2004.

*Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*. GAO-04-483T. Washington, D.C.: March 16, 2004.

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. GAO-04-354. Washington, D.C.: March 15, 2004.

*Information Security: Technologies to Secure Federal Systems*. GAO-04-467. Washington, D.C.: March 9, 2004.

*Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services*. GAO-04-160. Washington, D.C.: February 27, 2004.

*Information Security: Further Efforts Needed to Address Serious Weaknesses at USDA*. GAO-04-154. Washington, D.C.: January 30, 2004.

*Information Security: Improvements Needed in Treasury's Security Management Program*. GAO-04-77. Washington, D.C.: November 14, 2003.

*Information Security: Computer Controls over Key Treasury Internet Payment System*. GAO-03-837. Washington, D.C.: July 30, 2003.

*Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD*. GAO-03-1037T. Washington, D.C.: July 24, 2003.

*Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*. GAO-03-852T. Washington, D.C.: June 24, 2003.

*Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks*. GAO-03-44. Washington, D.C.: May 30, 2003.

*High-Risk Series: An Update*. GAO-03-119. Washington, D.C.: January 2003.

*Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk*. GAO-03-303T. Washington, D.C.: November 19, 2002.

## GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

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

## Public Affairs

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