United States Government Accountability Office

GAO

Testimony
Before the House Committee on
Government Reform

**For release on delivery
expected at 10:00 a.m. EDT
Thursday, April 7, 2005**

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-05-483T

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IG	inspector general
IT	information technology
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
NIST	National Institute of Standards and Technology

April 2005

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-05-483T, a testimony before the House Committee on Government Reform.

Why GAO Did This Study

For many years, GAO has reported that poor information security is a widespread problem that has potentially devastating consequences. Further, since 1997, GAO has identified information security as a governmentwide high-risk issue in reports to Congress—most recently in January 2005.

Concerned with accounts of attacks on commercial 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 of 2002 (FISMA), which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

This testimony discusses:

- The federal government's progress and challenges in implementing FISMA as reported by the Office of Management and Budget (OMB), the agencies, and Inspectors General (IGs).
- Opportunities for improving the usefulness of the annual reporting process, including the consideration of a common framework for the annual FISMA reviews conducted by the IGs.

www.gao.gov/cgi-bin/getrpt?GAO-05-483T.

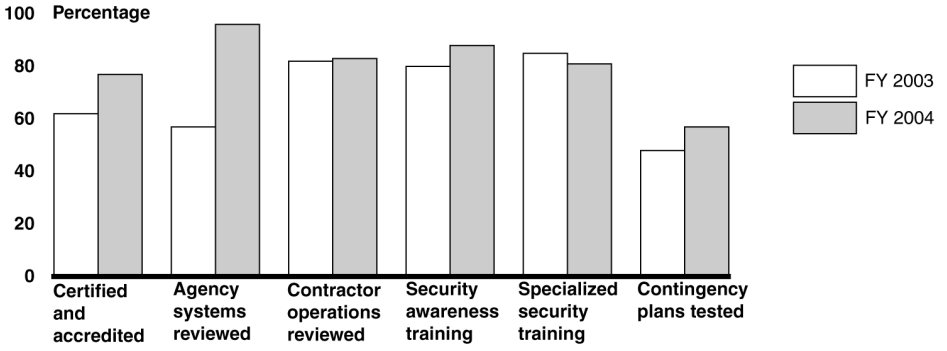
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-3317 or wilshuseng@gao.gov.

What GAO Found

In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long-standing problems, but at the same time, cites challenging weaknesses that remain. The report notes several governmentwide findings, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation (the process of authorizing operation of a system including the development and implementation of risk assessments and security controls). Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003 (see figure). Nevertheless, challenges remain. For example, only 7 agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and 6 of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems.

Opportunities exist to improve the usefulness of the annual FISMA reporting process, including enhancing the reliability and quality of reported information, providing performance information based on the relative importance or risk of the systems, and reporting on key information security requirements. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.

Percentage of Selected Performance Measurement Data for 24 Federal Agencies



Source: OMB's FY2003 and 2004 Report to Congress on Federal Government Information Security Management; GAO (analysis).

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss efforts by federal agencies and the administration to implement requirements of the Federal Information Security Management Act of 2002 (FISMA).[1] For many years, we have reported that poor information security is a widespread problem that has potentially devastating consequences.[2] Further, since 1997, we have identified information security as a governmentwide high-risk issue in reports to the Congress—most recently in January 2005.[3] Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made them vulnerable to attack, Congress passed FISMA, which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

In my testimony today, I will summarize the reported status of the federal government's implementation of FISMA and the efforts by 24 major federal agencies[4] to implement federal information security requirements, including areas of progress and continuing challenges. I will also present opportunities for improving the usefulness of annual reporting on FISMA implementation.

[1]*Federal Information Security Management Act of 2002*, *Title III*, *E-Government Act of 2002*, Pub. L. No. 107-347, Dec. 17, 2002.

[2]GAO, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

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

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

In conducting this review, we reviewed and summarized OMB's fiscal year 2004 report to Congress on FISMA implementation.[5] We also reviewed and summarized the fiscal year 2004 FISMA reports for 24 of the largest federal agencies and their Inspectors General (IGs). In addition, we reviewed standards and guidance issued by OMB and the National Institute of Standards and Technology (NIST) pursuant to their FISMA responsibilities. We did not validate the accuracy of the data reported by the agencies or OMB, but did analyze the IGs' fiscal year 2004 FISMA reports to identify any issues related to the accuracy of agency-reported information. We performed our work from October 2004 to March 2005 in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2004 report to the Congress, OMB noted that the federal government continued to make significant progress in identifying and addressing its security weaknesses, but that challenging weaknesses remain. In particular, the report identified several common deficiencies, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation processes.[6] The report also presented a plan of action that OMB is pursuing with agencies to improve performance.

In their fiscal year 2004 reports, the 24 major federal agencies generally reported an increasing number of systems meeting key statutory information security requirements, such as percentage of systems certified and accredited, number of systems and contractor operations reviewed annually, the percentage of employees and

[5]Office of Management and Budget, Federal Information Security Management Act (FISMA) 2004 Report to Congress, March 1, 2005.

[6]Certification is a comprehensive process of assessing the level of security risk, identifying security controls needed to reduce risk and maintain it at an acceptable level, documenting security controls in a security plan, and testing controls to ensure they operate as intended. Accreditation is a written decision by an agency management official authorizing operation of a particular information system or group of systems.

contractors who received security training, and the percentage of systems with contingency plans tested. Nevertheless, challenges remain. For example, 17 agencies reported that they had tested contingency plans for less than 90 percent of their systems.

Opportunities exist to improve the usefulness of the annual FISMA reporting process, including enhancing the reliability and quality of reported information, completing and reporting accurate system inventories, providing performance information based on the relative importance or risk of the systems, reporting on key information security requirements, and clarifying reporting instructions in areas such as inventory and remediation plans. In addition, a commonly accepted framework for the annual FISMA reviews conducted by the IGs could help ensure consistency and usefulness of their evaluations.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, without proper safeguards, this widespread interconnectivity also poses significant risks to the government's computer systems and, more importantly, to the critical operations and infrastructures they support.

We recently reported that while federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses in federal computer systems that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at the risk of disruption. The significance of these weaknesses led GAO to conclude in the audit of the federal government's fiscal year 2004

financial statements[7] that information security was a material weakness.[8] Our audits also identified instances of similar types of weaknesses in non-financial systems. Weaknesses continued to be reported in each of the six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

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

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of industrial espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud, identity theft, or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct

[7]U.S. Department of the Treasury, *2004 Financial Report of the United States Government* (Washington, D.C.; 2005).

[8]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.

operations and fulfill their fiduciary responsibilities.

Congress and the administration have established specific information security requirements in both law and policy to help protect the information and information systems that support these critical operations and assets.

FISMA Authorized and Strengthened Information Security Requirements

Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA authorized and strengthened information security program, evaluation, and reporting requirements. FISMA assigns specific responsibilities to agency heads, chief information officers, and IGs. It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing at least annually, and approving or disapproving, agency information security programs.

Overall, FISMA requires each agency (including agencies with national security systems) to develop, document, and implement an agencywide information security program. This program should provide information 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;
- 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 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 that are 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.

Each agency is also required to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency IG or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

The agencies are to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, practices, and compliance with FISMA requirements. In addition, agency heads are required to make annual reports of the results of their independent evaluations to OMB. OMB is also required to submit a report to Congress no later than March 1 of each year on agency compliance, including a summary of the findings of agencies' independent evaluations.

Other major provisions require the National Institute of Standards and Technology (NIST) to develop, 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 and guidelines, developed in conjunction with the Department of Defense and the National Security Agency, for identifying an information system as a national security system.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

Consistent with FISMA requirements, OMB issues guidance to the agencies on their annual reporting requirements. 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 formatted these instructions to emphasize a quantitative rather than a narrative response. OMB has developed performance measures in the following areas:

- certification and accreditation
- testing of security controls
- agency systems and contractor operations or facilities reviewed annually
- annual security awareness training for employees
- annual specialized training for employees with significant security responsibilities
- testing of contingency plans
- minimum security configuration requirements
- incident reporting

Further, OMB provided instructions for continued agency reporting on the status of remediation efforts through plans of action and

milestones. Required for all programs and systems where an IT security weakness has been found, these plans 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. The plans are to be submitted twice a year. In addition, agencies are to submit quarterly updates that indicate the number of weaknesses for which corrective action was completed on time (including testing), is ongoing and on track to be completed as originally scheduled, or has been delayed, as well as the number of new weaknesses discovered since the last update.

The IGs' reports were to be based on the results of their independent evaluations, including work performed throughout the reporting period (such as financial statements or other audits). While OMB asked the IGs to respond to the same questions as the agencies, it also asked them to assess whether their agency had developed, implemented, and was managing an agencywide plan of actions and milestones. Further, OMB asked the IGs to assess the certification and accreditation process at their agencies. OMB did not request that the IGs validate agency responses to the performance measures. Instead, as part of their independent evaluations of a subset of agency systems, IGs were asked to assess the reliability of the data for those systems that they evaluated.

OMB Report to Congress Noted Progress and Challenges

In its March 1, 2005, report to Congress on fiscal year 2004 FISMA implementation,[9] OMB concluded that the federal government continued to make significant progress in identifying and addressing its security weaknesses but that much work remains. OMB assessed the agencies in their progress against three governmentwide security goals established in the President's 2004 budget:

[9]Office of Management and Budget, *Federal Information Security Management Act (FISMA): 2004 Report to Congress* (Washington, D.C.: Mar. 1, 2005).

- *Goal 1 — As required by FISMA, all federal agencies are to have created a central remediation process to ensure that program and system-level IT security weaknesses, once identified, are tracked and corrected. In addition, each agency IG is to verify whether the agency has a process in place that meets criteria specified in OMB guidance.* Based on IG responses to these criteria, OMB reported that each agency had an IT security remediation process, but that the maturity of these processes varied greatly. They did note that 18 agencies now have a remediation process verified by the IG, up from 12 in 2003.
- *Goal 2 — Eighty percent of federal IT systems are to be certified and accredited.* Although agencies have not reached this goal, they did come close, certifying and accrediting 77 percent of their systems.
- *Goal 3 — Eighty percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the life cycle of the investment.* OMB reported that agencies have exceeded this goal by integrating security into the life cycle of 85 percent of their systems.

OMB also noted that, while progress has been made, deficiencies in security policy, procedure and practice continue to be identified at the agencies. Common deficiencies noted by OMB in its report were:

- *Agencywide plans of action and milestones*. Agencies had not fully implemented plans of action and milestones. The OMB report noted that IGs assessed the quality of their agencies' remediation process during 2004 and that six IGs identified overall deficiencies in their agencies' processes.
- *Quality of certification and accreditation process*. Agencies' certification and accreditation processes were inconsistent in quality. Fifteen IGs rated the agency process as good or satisfactory; however, seven IGs rated the process as poor and two did not report because they did not complete the evaluation.
- *Assessment of agency incident handling programs*. Agencies were not reporting security incidents consistently. OMB noted that agencies are required to notify and consult with the federal information security incident center operated by the Department of Homeland Security. However, the department's statistics indicate

sporadic security incident reporting by some agencies and unusually low levels of reported malicious activity at other agencies.

The report also outlined a plan of action to improve performance, assist agencies in their information technology security activities, and promote compliance with statutory and policy requirements. OMB has set a goal for agencies, that by June 2005 they will have all systems certified and accredited, have systems installed and maintained in accordance with security configurations, and have consolidated all agency infrastructure to include providing for continuity of operations.

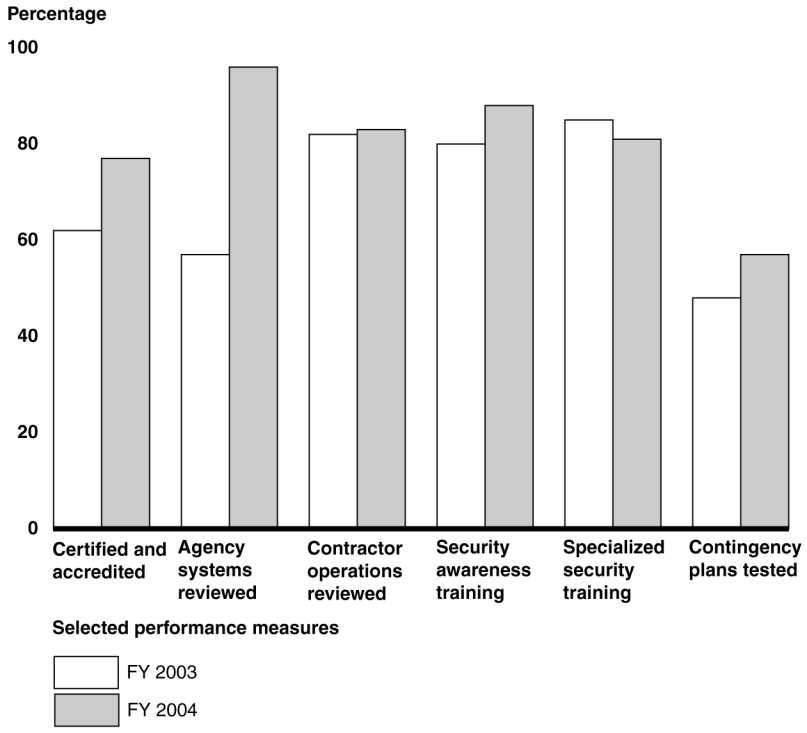
Agency FISMA Reports Highlight Increases in Performance Measures, but Challenges Remain

In their FISMA-mandated reports for fiscal year 2004, the 24 major agencies generally reported increases in their compliance with information security requirements as compared with 2003. However, analysis of key measures revealed areas where agencies face challenges. The following key measures showed increased performance and/or continuing challenges:

- percentage of systems certified and accredited;
- percentage of agency systems reviewed annually;
- percentage of contractor operations reviewed annually;
- percentage of employees receiving annual security awareness training;
- percentage of employees with significant security responsibilities receiving specialized security training annually; and
- percentage of contingency plans tested.

Figure 1 illustrates the reported overall status of the 24 agencies in meeting these performance measures and the increases between fiscal years 2003 and 2004. Summaries of the results reported for the specific measures follow.

Figure 1: Reported Performance Measurement Data for Selected Performance Measures for the 24 Major Agencies



Source: OMB's FY2003 and 2004 Report to Congress on Federal Government Information Security Management; GAO (analysis).

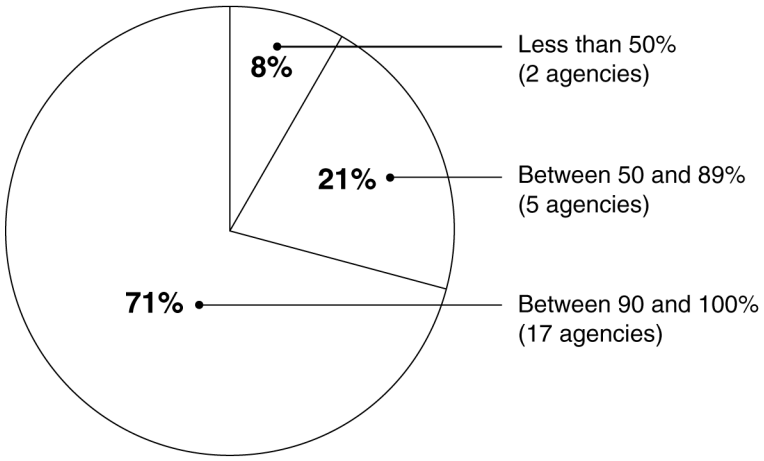
Certification and Accreditation

Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. For FISMA reporting, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation.

Data reported for this measure showed overall increases for most agencies. For example, 19 agencies reported an increase in the percentage of their systems that had completed certification and

accreditation. Overall, 77 percent of the agencies' systems governmentwide were reported as certified and accredited, compared to 62 percent in 2003. In addition, 17 agencies reported 90 percent or more of their systems had successfully completed the process, as illustrated in figure 2.

Figure 2: Percentage of Systems during Fiscal Year 2004 that are Authorized for Processing after Certification and Accreditation



Source: Agency-reported data and GAO (analysis).

However, as we previously reported, our analysis of the certification and accreditation of 32 selected systems at four agencies[10] identified instances where appropriate criteria were not always met. For example, we noted instances in which systems were accredited even though risk assessments were outdated, contingency plans were incomplete or untested, and control testing was not performed. Further, in some cases, documentation did not clearly indicate what residual risk the accrediting official was actually accepting in making the authorization decision. As such, agency reported performance data may not accurately reflect the status of an agency's efforts to implement this requirement.

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

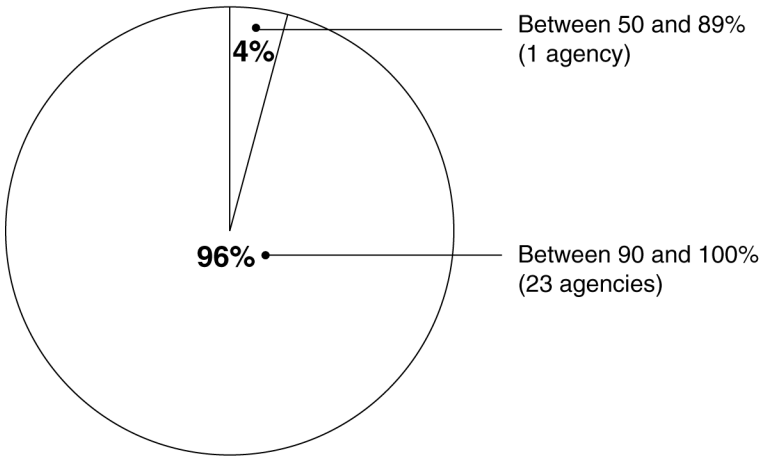
The information reported for certification and accreditation has taken on new importance this year as OMB has changed the reporting requirements for 2004. In 2003, agencies were required to report separately on risk assessments and security plans. In 2004, OMB eliminated this separate reporting in its guidance and directed agencies to complete risk assessments and security plans for the certification and accreditation process to be accomplished. As a result, the performance measure for certification and accreditation now also reflects the level of agency compliance for risk assessments and security plans.

Annual Review of Agency Systems

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 cost effectively, 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 GAO audits to help provide a more complete picture of the agencies' security postures. As a performance measure for this requirement, OMB requires that agencies report the number of systems that they have reviewed during the year.

Agencies reported a significant increase in the percentage of their systems that underwent an annual review. Twenty-three agencies reported in 2004 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 figure 3).

Figure 3: Percentage of Systems Reviewed During Fiscal Year 2004



Source: Agency-reported data and GAO (analysis).

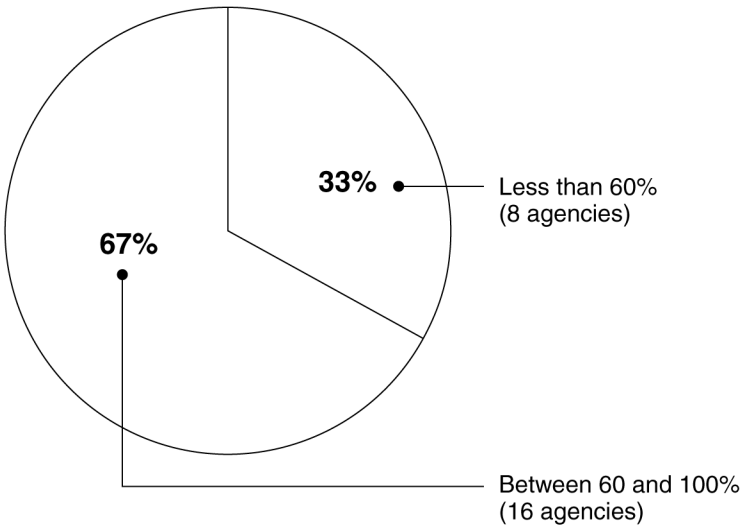
Annual security testing helps to provide assurance to the agencies that security controls are in place and functioning correctly. Without such testing, agencies cannot be assured that their information and systems are protected.

Annual Review of Contractor Operations

Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. Thus, as OMB emphasized in its fiscal year 2003 FISMA reporting guidance, agency IT security programs apply to all organizations that possess or use federal information or that operate, use, or have access to federal information systems on behalf of a federal agency. Such other organizations may include contractors, grantees, state and local governments, and industry partners. This underscores longstanding OMB policy concerning sharing government information and interconnecting systems: federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

The key performance measure of annually reviewing contractor operations showed a minor increase from 80 percent in 2003 to 83 percent in 2004. Although there was an increase overall, 8 agencies reported reviewing less than 60 percent of their contractor systems, twice the number of agencies reporting that level in 2003. The breakdown of the percentages of contractor operations reviewed by agency is provided in figure 4.

Figure 4: Percentage of Contractor Operations Reviewed during Fiscal Year 2004



Source: Agency-reported data and GAO (analysis).

Security Awareness Training

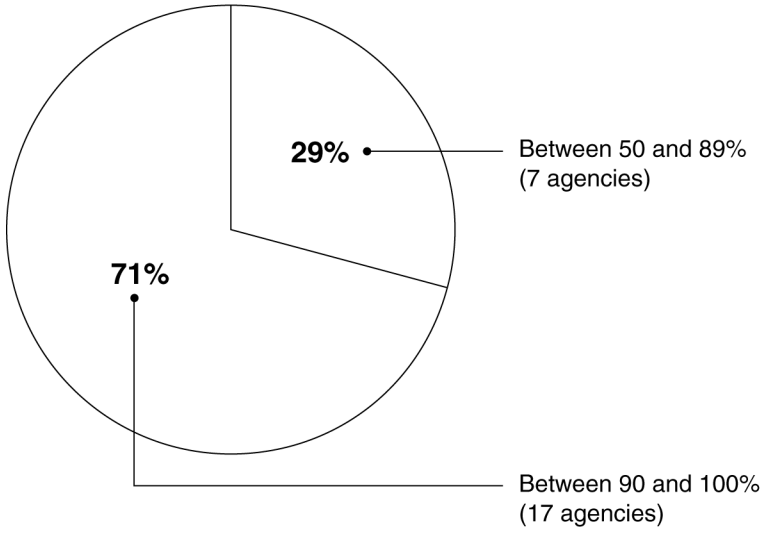
FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading organizations[11] have shown that such

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

organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. Agencies reported that they provided security awareness training to the majority of their employees and contractors. As performance measures for FISMA training requirements, OMB has the agencies report the number of employees and contractors who received IT security training during fiscal year 2004.

The majority of agencies reported increases in the number of individuals who had received basic security awareness training. Seventeen agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness (see figure 5).

Figure 5: Percentage of Employees and Contractors who Received IT Security Awareness Training in Fiscal Year 2004



Source: Agency-reported data and GAO (analysis).

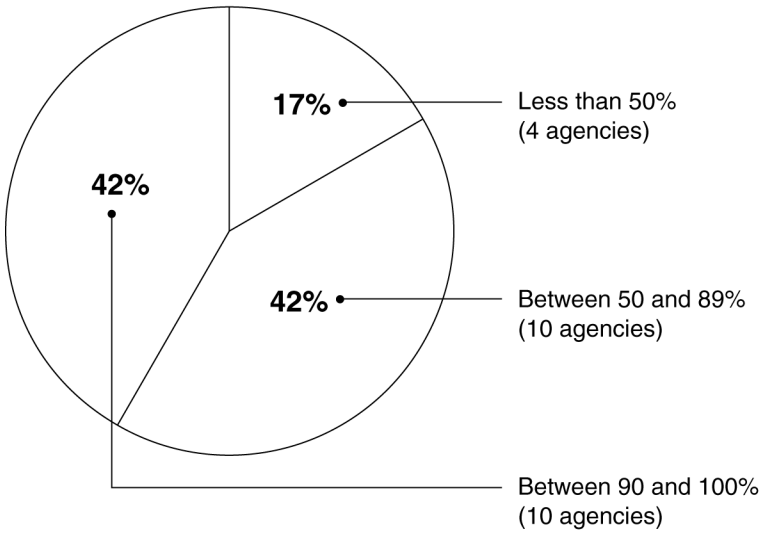
That figure represents an improvement over 2003, when only 13 agencies reported a 90 percent or higher rate.

Specialized Security Training

Under FISMA, agencies are required to provide training in information security to personnel with significant security responsibilities. As previously noted, our study of best practices at leading organizations have shown that such organizations recognized that staff expertise needed to be updated frequently to keep security employees updated on changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. OMB directs agencies to report on the percentage of their employees with significant security responsibilities who received specialized training.

Agencies reported varying levels of compliance in providing specialized training to employees with significant security responsibilities. Ten agencies reported that they had provided specialized security training for 90 percent or more of these employees (see figure 6).

Figure 6: Percentage of Employees with Significant Security Responsibilities Who Received Specialized Security Training in Fiscal Year 2004



Source: Agency-reported data and GAO (analysis).

Note: Total does not add to 100 percent due to rounding

Moreover, 10 agencies reported a decrease in the number of such employees who received specialized training. Given the rapidly changing threats in information security, agencies need to keep their IT security employees up-to-date on changes in technology. Otherwise, agencies may face increased risk of security breaches.

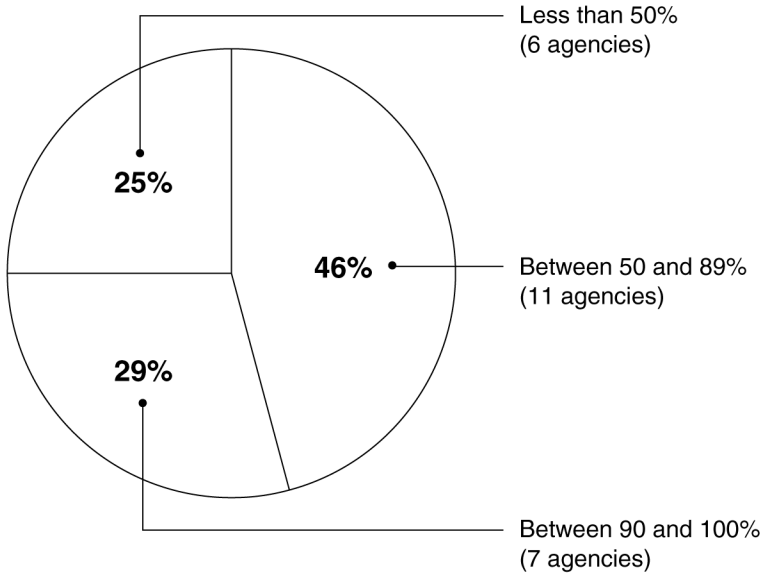
Testing of Contingency Plans

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, and the frequency of plan testing will vary depending on the criticality of the entity's operations. The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data 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 requires that agencies report the number of systems that have a contingency plan and the number that have contingency plans that have been tested.

Agencies' reported fiscal year 2004 data for these measures showed that although 19 agencies reported increases, 6 agencies reported less than 50 percent of their systems had tested contingency plans (see figure 7).

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



Source: Agency-reported data and GAO (analysis).

Overall, federal agencies reported that 57 percent of their contingency plans had been tested. Without testing, agencies can have limited assurance that they will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption.

Opportunities Exist to Increase Usefulness of Annual Reporting

Periodic reporting of performance measures for FISMA requirements and related analysis is providing valuable information on the status and progress of agency efforts to implement effective security management programs, thereby assisting agency management, OMB, and Congress in their management and oversight roles. Several opportunities exist to improve the usefulness of such information as indicators of both governmentwide and agency-specific performance in implementing information security requirements. In developing future reporting guidance, OMB can consider how their efforts can help to address

the following factors that affect the usefulness of the current annual reporting process.

- *Limited assurance of data reliability.* Currently, there is limited assurance of the accuracy of the data reported in the performance measures. The performance measures reported by the agencies are primarily based on self-assessments and are not independently verified. OMB did not require the IGs to verify agency responses to the performance measures. In addition, OMB does not require agency officials to attest to the accuracy of agency-reported performance data. In the absence of independent verification of data, such a statement could provide additional assurance of the data's accuracy.

- *Limited assurance of the quality of agency processes.* The performance measures offer limited assurance of the quality of the agency processes that generate the data. For example, the agencies report on the number of agency systems and contractor operations that they review annually. They also report on, and the IGs confirm, whether they used appropriate guidance. However, there is no reporting on the quality of the reviews, including whether guidance was applied correctly or if the results are tracked for remediation. OMB has recognized the need for assurance of quality for some agency processes. For example, it specifically requested the IGs to evaluate the plan of action and milestones process and the certification and accreditation process at their agencies. The results of these evaluations call into question the reliability and quality of the performance data reported by several agencies. As a result, increased risk exists that the performance data reported by the agencies may not be reliable or accurate.

- *Accuracy of agency system inventories.* Accurate inventory data would increase reliability of the reporting measures. While significantly more agencies reported having accurate inventories in the 2004 reports than in 2003, four agencies reported that they did not have accurate inventories. 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 affects the

percentage of systems shown as meeting the requirements. Further, a complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. Twenty agencies reported having inventories of their major systems in their 2004 reports, whereas in 2003 only 13 agencies responded affirmatively. However, 16 IGs reported that they did not agree with the accuracy of their agency's inventory. Without reliable information on agencies' inventories, the agencies, the administration, and Congress can not be fully assured of agencies' progress in implementing FISMA.

- *Data reported in aggregate, not according to agency risk.* Performance measurement data are reported on the total number of agency systems but do not indicate the relative importance or risk of the systems for which FISMA requirements have been met. The Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[12] requires agencies to categorize their information systems according to 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). Reporting information by system risk would provide better 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' most important systems. Therefore, agencies, the administration, and Congress cannot be sure that critical federal operations can be restored if an unexpected event disrupts service.

- *Reporting on key FISMA requirements.* 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

[12]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199, December 2003.

incidents internally to law enforcement and to the U.S. Computer Emergency Readiness Team at the Department of Homeland Security. 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 security incident handling capabilities. The annual reporting process does not include separate reporting on key FISMA requirements. For example, in the 2004 guidance, OMB eliminated separate reporting on risk assessments and security plans. Because NIST guidance on the certification and accreditation process requires both risk assessments and security plans, OMB did not require agencies to answer separate questions on risk assessments and security plans. Although OMB asked for the IGs' assessment of the certification and accreditation process, it did not require them to comment on these specific requirements.

- *Clear reporting instructions.* Several questions in OMB's 2004 reporting guidance relating to agency inventories, plans of action and milestones, certification and accreditation process, and system configuration requirements 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 was not using the plan, or that one of them was not using the plan. Discussions with agency officials and IGs and our analysis of their annual reports indicate that they interpreted several questions differently. Another example 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 the agency's categorization. Alternatively, a negative response could mean that the IG disagreed with the overall accuracy of the inventory. Clarifying reporting instructions could increase the reliability and consistency of reported performance data.

- *Accepted framework for IG reviews.* A commonly accepted framework for the annual reviews conducted by the IGs under FISMA could help ensure the consistency and usefulness of their evaluations. Because a commonly accepted framework currently does not exist for the IGs, they do not have a common methodology. This inconsistency can affect the consistency and comparability of reported results, potentially reducing the usefulness of the IG reviews for assessing the governmentwide information security posture. The IG community has recognized the importance of this issue. Working through the President's Council on Integrity and Efficiency, the IGs are working to develop a framework for FISMA reviews. They are including both OMB and GAO in their deliberations. The President's Council on Integrity and Efficiency is composed of IGs who are appointed by the President. The Council currently maintains *The Financial Audit Manual* in cooperation with GAO, which brings expertise and experience to the development of a FISMA review framework.

In summary, through the continued emphasis of information security by the Congress, the administration, agency management, and the audit community, the federal government has seen improvements in its information security. However, despite the progress shown by increases in key performance measures, challenges still exist. Accordingly, if information security is to continue to improve, agency management must remain committed to these efforts. The annual reports and performance measures will continue to be key tools for holding agencies accountable and providing a barometer of the overall status of federal information security. It is therefore essential that agencies' monitoring, review, and evaluation processes provide Congress, the administration, and IG and agency management with assurance that these measures accurately reflect agency progress.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the Committee may have at this time.

Should you have any questions about this testimony, please contact me at (202) 512-3317 or Suzanne Lightman, Assistant Director, at

(202) 512-8146. We can also be reached by e-mail at wilshuseng@gao.gov and lightmans@gao.gov, respectively.

Other individuals making key contributions to this testimony include Larry Crosland, Season Dietrich, Nancy Glover, Carol Langelier, and Stephanie Lee.

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