United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 1:00 p.m. EST
Tuesday, March 16, 2004

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

Statement of Robert F. Dacey
Director, Information Security Issues

March 16, 2004

INFORMATION SECURITY

Continued Efforts Needed To Sustain Progress in Implementing Statutory Requirements

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-483T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Goverment Reform

Why GAO Did This Study

For many years, GAO has reported on the widespread negative impact of poor information security within federal agencies and has identified it as a governmentwide high-risk issue since 1997. Legislation designed to improve information security was enacted in October 2000. It was strengthened in December 2002 by new legislation, the Federal Information Security Management Act of 2002 (FISMA), which incorporated important new requirements.

This testimony discusses

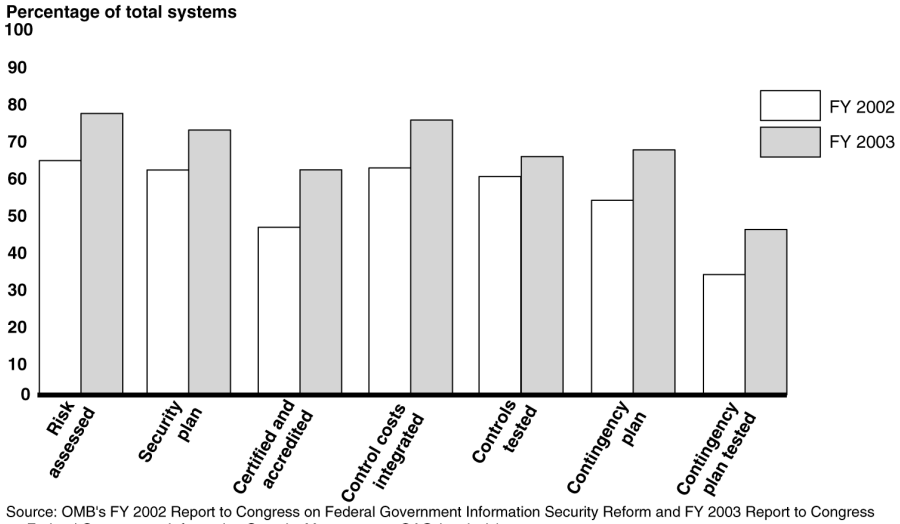
- the Office of Management and Budget's (OMB) recent report to the Congress required by FISMA on the government's overall information security posture,
- the reported status of efforts by 24 of the largest agencies to implement federal information security requirements,
- opportunities for improving the usefulness of performance measurement data, and
- progress by the National Institute of Standards and Technology (NIST) to develop related standards and guidance.

What GAO Found

OMB reports significant strides in addressing long-standing problems, but at the same time cites challenging weaknesses that remain. One governmentwide weakness OMB emphasizes is a lack of understanding—and therefore accountability—on the part of agency officials regarding their responsibilities for ensuring the security of information and systems. The report presents a plan of action to close these gaps through both management and budgetary processes.

Fiscal year 2003 FISMA data showed that, overall, the 24 federal agencies reported increasing numbers of their systems met the information security requirements represented by key OMB performance measures. For example, of the total number of systems reported by these agencies, the reported number assessed for risk climbed from 65 percent to 78 percent, those having a contingency plan jumped from 55 to 68 percent, and those authorized for processing following certification and accreditation rose from 47 to 62 percent (see chart). However, reported results varied widely among individual agencies, with some reporting that less than half of their systems met certain requirements. Further, GAO noted opportunities to improve the usefulness of reported performance management data, including independent validation of these data and completion of system inventories.

Reported Performance Measurement Data for Selected Information Security Requirements for 24 Large Federal Agencies



Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

NIST made progress in developing security-related standards and guidance required by FISMA. These include standards to categorize systems according to potential impact in the event of a security breach and recommended controls for such systems. However, according to NIST, current and future funding constraints could threaten its information security work.

www.gao.gov/cgi-bin/getrpt?GAO-04-483T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts by federal departments and 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 with 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 2003.[3]

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, in October 2000 the Congress passed and the President signed into law the Government Information Security Reform provisions (commonly known as GISRA) to strengthen information security practices throughout the federal government.[4] With GISRA expiring in November 2002, FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies by GISRA. FISMA added important new requirements, such as mandating that the National Institute of Standards and Technology (NIST) develop minimum information security requirements for information systems.

In my testimony today, I will summarize the federal government's overall information security progress and challenges as discussed in the Office of Management and Budget's (OMB) report to the Congress on fiscal year 2003 FISMA implementation released on March 1, 2004.[5] I will also discuss the reported status of efforts by 24 of the largest federal agencies to

[1] *Federal Information Security Management Act of 2002*, *Title III*, *E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

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

[3] U.S. General Accounting Office, *High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

[4] *Title X, Subtitle G—Government Information Security Reform*, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L.106-398, October 30, 2000.

[5] Office of Management and Budget, *FY 2003 Report to Congress on the Federal Government Information Management*, March 1, 2004.

implement federal information security requirements, as well as opportunities for improving the usefulness of agency-reported FISMA performance measurement data.[6] I will then discuss actions being taken by NIST in meeting its FISMA requirements to develop information-security-related standards and guidance.

In conducting this review, we reviewed and summarized the fiscal year 2003 FISMA reports for 24 of the largest federal agencies and their inspectors general (IGs). In addition, we reviewed standards and guidance issued by NIST pursuant to its FISMA responsibilities and discussed the progress of these efforts with NIST officials. We also reviewed and summarized OMB's March 2004 report to the Congress on FISMA implementation. We did not validate the accuracy of the data reported by the agencies or OMB, but did analyze the IGs' fiscal year 2003 FISMA reports to identify any issues related to the accuracy of FISMA-reported information. We performed our work from October 2003 to March 2004, in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2003 report to the Congress, OMB notes that the federal government has made significant strides in identifying and addressing long-standing problems, but that challenging weaknesses remain. In particular, the report notes several governmentwide findings, such as limited progress against governmentwide information security milestones and a lack of clear accountability for ensuring security of information and systems. The report also presents a plan of action that OMB is pursuing with agencies to close those gaps and improve the security of federal information and systems. Planned actions include prioritizing agencies' information technology (IT) spending to resolve security weaknesses and improving the federal government's incident prevention and management

[6]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. These agencies exclude the Federal Emergency Management Agency, which is now within the new DHS. DHS also incorporated components of other agencies, including the U.S. Coast Guard and U.S. Customs Service, that were formerly within the Departments of Transportation and the Treasury, respectively.

capabilities to respond to the increasing number and potential impact of threats and vulnerabilities.

Fiscal year 2003 data reported by the 24 large agencies for a subset of OMB's performance measures show increasing numbers of systems meeting the statutory information security requirements represented by these measures compared with fiscal year 2002. For example, the total number of systems that had been assessed for risk increased by 13 percentage points to 78 percent. Other reported key measures, such as the percentage of systems with up-to-date security plans, also showed increases ranging from 4 to 15 percentage points.

Agencies' fiscal year 2003 FISMA reports showed that performance measures for many agencies have increased, but there are wide variances among the agencies. For example, compared with last year's results, 17 agencies reported increases in the percentage of systems authorized for processing after certification and accreditation—a process that OMB considers an important information security quality control.[7] However, only 6 agencies reported that they had authorized 90 to 100 percent of their systems, and 11 of the remaining 18 agencies reported that they had authorized less than half of their systems. Moreover, the IGs' evaluations, as well as our own ongoing review, have identified deficiencies in agencies' certifications and accreditations, such as lack of control testing and outdated risk assessments. We also noted several opportunities to improve the usefulness of reported performance management data, including independent validation of reported information, completion of system inventories, and providing performance information based on the relative importance or risk of the systems.

[7]*Certification* is the comprehensive evaluation of the technical and nontechnical security controls of an IT system that provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. This management approval, or *accreditation*, is the authorization of an IT system to process, store, or transmit information that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation decision is based on the implementation of an agreed-upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it. Agencies are required to reaccredit their systems prior to a significant change in processing, but at least every 3 years (more often where there is a high risk and potential magnitude of harm).

For its part, NIST has taken a number of actions to develop security-related standards and guidance required by FISMA. These include the issuance of standards to categorize federal information and information systems according to levels of potential impact on organizational operations, assets, or individuals, should a breach of security occur. However, according to NIST, current and future funding constraints could affect its information security and critical infrastructure protection work, including providing guidance and other assistance to agencies to improve their information security.

Background

Our recent analyses of audit results for federal agencies showed improvement, but continued to show significant weaknesses in federal computer systems that put critical 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 risk of disruption. The significance of these weaknesses led GAO to recently conclude that information security was a material weakness in our audit of the federal government's fiscal year 2003 financial statements.[8] Audits also identified instances of similar types of weaknesses in non-financial systems, which continue to receive increased audit coverage in response to FISMA requirements. 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. These six areas are (1) security program management, a principal focus of FISMA, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, also

[8]U.S. General Accounting Office, *Fiscal Year 2003 U.S. Government Financial Statements: Sustained Improvement in Federal Financial Management Is Crucial to Addressing Our Nation's Future Fiscal Challenges*, GAO-04-477T (Washington, D.C.: March 3, 2004).

addressed by FISMA, which ensures that computer-dependent operations experience no significant disruptions.

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 extremely 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 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 or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct 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.

FISMA Permanently Authorizes and Strengthens Information Security Requirements

On October 30, 2000, Congress passed GISRA, which was signed into law and became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and

the Clinger-Cohen Act of 1996 and was consistent with existing information security guidance issued by OMB[9] and NIST,[10] as well as audit and best practice guidance issued by GAO.[11] Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA permanently authorized and strengthened GISRA's information security program, evaluation, and reporting requirements. Like GISRA, FISMA assigns specific responsibilities to agency heads, chief information officers (CIO), 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. FISMA continues to delegate OMB responsibilities for national security systems to the Secretary of Defense and the Director of Central Intelligence.

Overall, FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to 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;

[9]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[10]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.

[11]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- 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 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.

The law also requires an agency's CIO to designate a senior agency information security officer who, for the agency's FISMA-prescribed information security responsibilities, shall

- carry out the CIO's responsibilities;

- possess professional qualifications, including training and experience, required to administer the required functions;

- have information security duties as that official's primary duty; and
- head an office with the mission and resources to assist in ensuring agency compliance.

Under FISMA, each agency must continue 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.

FISMA requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices, and compliance with FISMA's requirements. In addition, agency heads are required to annually report the results of their independent evaluations to OMB, except that to the extent an evaluation pertains to a national security system, only a summary and assessment of that portion of the evaluation is reported to OMB. OMB is also required to submit a report to the Congress no later than March 1 of each year on agency compliance with FISMA's requirements, including a summary of findings of agencies' independent evaluations. FISMA also requires the Comptroller General to periodically evaluate and report to Congress on (1) the adequacy and effectiveness of agency information security policies and practices and (2) implementation of FISMA requirements.

Other major FISMA provisions require 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.

The law also assigned 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;
- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;
- developing and periodically revising performance indicators and measures for agency information security policies and practices;
- 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
- periodically assessing the effectiveness of and revising, as appropriate, the NIST standards and guidelines developed under FISMA.

NIST is required to prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out its responsibilities under FISMA.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

On August 6, 2003, OMB issued its fiscal year 2003 FISMA reporting instructions and guidance on quarterly IT security reporting.[12] These instructions, which required agencies to submit their reports to OMB by September 22, 2003, essentially continued many of the reporting requirements established for GISRA, including performance measures introduced for fiscal year 2002 reporting under that law. The instructions also highlighted the more substantive changes introduced by FISMA. For example, OMB emphasized that FISMA applies to both information and information systems used by an agency and by its contractors or other organizations and sources that possess or use federal information or that operate, use, or have access to federal information systems. OMB also

[12]Office of Management and Budget, "*Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*," Memorandum for Heads of Executive Departments and Agencies, Joshua B. Bolten, Director, M-03-19, August 6, 2003.

underscored that FISMA requires each agency to test and evaluate the effectiveness of the information security policies, procedures, and practices for each system at least annually.

OMB's fiscal year 2003 reporting instructions also emphasized the strong focus on performance measures and formatted these instructions to emphasize a quantitative rather than a narrative response. OMB also required agencies to provide quarterly updates for a key subset of these performance measures, with the first update due December 15, 2003. Measures within this key subset are the numbers of systems that have

- risk assessments and assigned levels of risk,
- up-to-date IT security plans,
- certifications and accreditations,
- security control costs integrated into their life cycles,
- security controls tested and evaluated in the last year,
- contingency plans, and
- contingency plans tested.

Further, OMB provided instructions for continued agency reporting on the status of remediation efforts through plans of action and milestones (POA&M). Required for all programs and systems where an IT security weakness has been found, a POA&M 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. POA&Ms are to be submitted twice a year. In addition, agencies are to submit quarterly updates that show 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 new weaknesses discovered since that last update.

Consistent with last year, OMB's fiscal year 2003 guidance continued to authorize agencies to release certain information from their POA&Ms to assist the Congress in its oversight responsibilities. Agencies could release this information, as requested, excluding certain elements, such as estimated funding resources and the scheduled completion dates for resolving a weakness.

Lastly, as part of IG FISMA reporting, OMB instructed the IGs to respond to essentially the same questions that the agencies were to respond to in their reports. The IG responses were to be based on the results of their independent evaluations, including agency progress in implementing and maintaining their POA&Ms, and any other work performed throughout the reporting period (such as financial statement or other audits). This year, OMB also asked the IGs to assess against specific criteria whether the agency had developed, implemented, and was managing an agencywide POA&M process. OMB noted that this assessment was critical because effective remediation of IT security weaknesses is essential to achieving a mature and sound IT security program and securing information and systems. Further, OMB identified this IG assessment as one of the criteria used in evaluating agencies under the Expanding E-Government Scorecard of the President's Management Agenda.

OMB also instructed the IGs to use the performance measures to assist in evaluating agency officials' performance. However, it did not request them to validate agency responses to the performance measures. Instead, as part of their independent evaluations of a subset of agency systems, IGs were to assess the reliability of the data for those systems that they evaluated.

OMB's Report to Congress Notes Progress and Challenges

In its *FY 2003 Report to Congress on Federal Government Information Security Management*, published this month, OMB concludes that the federal government has made significant strides in identifying and addressing long-standing problems, but that challenging weaknesses remain. Overall, the report discusses the steps taken by OMB and federal agencies to implement FISMA, details progress made in fiscal year 2003, and identifies IT security gaps and weaknesses. The report also presents a plan of action that OMB is pursuing with agencies to close these gaps and improve the security of federal information and systems. This plan is intended to resolve information and security challenges through both management and budgetary processes.

OMB's report discussed four governmentwide findings:

1. *Agencies' Progress Against Governmentwide IT Security Milestones.* The President's fiscal year 2004 budget established three governmentwide goals to be met by the end of calendar year 2003. These goals and the progress reported against them were:

- 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 has an IT security remediation process, but that the maturity of these processes varies greatly. In particular, the report noted that for the 24 large agencies, only half have a remediation process verified by their IGs as meeting the necessary criteria.

- Goal 2 — Eighty percent of federal IT systems are to be certified and accredited. OMB reported that many agencies are not adequately prioritizing their IT investments to ensure that significant IT security weaknesses are appropriately addressed. As a result, at the end of 2003, the reported percentage of systems certified and accredited had increased to 62 percent, but was still short of the goal. Related to this goal, the report noted that most security weaknesses can be found in operational systems that either have never been certified and accredited or whose certification and accreditation are out of date.

- Goal 3 — Eighty percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment. OMB reported that agencies have made improvements in integrating security into new IT investments, but that significant problems remain, particularly in ensuring security of existing systems. As an example, the report provided results for the performance measure related to this goal, which showed that at the end of 2003, the percentage of systems that had integrated security into the lifecycle of the investment increased to 78 percent.

2. *Agency Progress Against Key IT Security Measures*. As the report highlights, because of GISRA and the OMB-developed performance measures, the federal government is now able to measure progress in IT security; and the Congress, OMB, the agencies, and GAO are able to track and monitor agency efforts against those measures. Noting agency progress, the report provides a table comparing results of 24 large federal agencies for key performance measures for fiscal years 2001, 2002, and 2003. However, it also notes that further work is needed, and uses the area of contingency planning as an example, where only 48 percent of the systems had tested contingency plans. A comparison of reported overall results for fiscal year 2002 and 2003 is provided below in table 1.

Table 1: Comparison of Fiscal Year 2002 and Fiscal Year 2003 Performance Measurement Data for 24 Large Federal Agencies

	Total		Assessed for risk and assigned a level of risk		Up-to-date IT security plan		Processing authorized following certification/ accreditation		Security control costs integrated into system life cycle		Security controls tested and evaluated in the last year		Have a contingency plan		Contingency plan tested	
Year	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**	**FY02**	**FY03**
Number of systems[a]	7,957	7,998	5,160	6,236	4,930	5,838	3,772	4,969	4,919	6,182	4,751	5,143	4,342	5,450	2,768	3,839
Percent of total systems			65	78	62	73	47	62	62	77	60	64	55	68	35	48
Difference from FY02 to FY03	+41 systems		+13 percentage points		+11 percentage points		+15 percentage points		+15 percentage points		+4 percentage points		+13 percentage points		+13 percentage points	

Source:OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

[a]Fiscal year 2002 totals include data for FEMA, which is now part of DHS.

3. *IGs' Assessment of Agency Plan of Action and Milestones Process.* As mentioned in the discussion of goal 1, OMB requested that IGs assess against a set of criteria whether the agency had a robust agencywide plan of action process. OMB reported the overall results of this assessment for the 24 agencies, which showed that 8 had such a process; 4 did, but with improvements needed; 11 did not; and one did not submit a report (DOD).

4. *Lack of Clear Accountability for Ensuring Security of Information and Systems*. The report emphasizes that even with the strong focus of both GISRA and FISMA on the responsibilities of agency officials regarding security, there continues to be a lack of understanding, and therefore, accountability within the federal government. Issues that continue to be a concern include the following:

- Agency and IG reports continue to identify the same IT security weaknesses year after year, some of which are seen as repeating material weaknesses.
- Too many legacy systems continue to operate with serious weaknesses.
- As a result, there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development.

In further discussing this finding, the report concludes that these concerns must be addressed through improved accountability, that is, holding agency program officials accountable for ensuring that the systems that support their programs and operations are secure. Further, it emphasizes that ensuring the security of an agency's information and systems is not the responsibility of a single agency official or the agency's IT security office, but rather a responsibility to be shared among agency officials that support their operations and assets.

The report also outlines a plan of action to improve performance that identifies specific steps it will pursue to assist agencies in their IT security activities, promote implementation of law and policy, and track status and progress. These steps are:

- *Prioritizing IT Spending to Resolve IT Security Weaknesses.* OMB reports that it used information from agencies' annual FISMA reports and quarterly POA&M updates in making funding decisions for fiscal year 2004, as well as for fiscal year 2005 to address longer term security weaknesses. For example, agencies with significant information and system security weaknesses were directed to remediate operational systems with weaknesses prior to spending fiscal year 2004 IT development or modernization funds. Further, if additional resources are needed to resolve those weaknesses, agencies are to use those fiscal year 2004 funds originally sought for new development.

- *President's Management Agenda Scorecard.* To "get to green" under the Expanding E-Government Scorecard for IT security, agencies are required to meet the following three criteria: (1) demonstrate consistent progress in remediating IT security weaknesses; (2) attain certification and accreditations for 90 percent of their operational IT systems; and (3) have an IG-assessed and IG-verified agency POA&M process.

- *Fiscal Year 2004 OMB FISMA Guidance.* OMB plans to further emphasize performance measurement in next year's guidance. In particular, its focus will center on three areas: (1) evolving the IT security performance measures to move beyond status reporting to also identify the quality of the work done, such as determining both the number of systems certified and accredited and the quality of certification and accreditation conducted; (2) further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes, such as remediation and intrusion detection and reporting; and (3) providing additional clarity to certain definitions to eliminate interpretation differences within agencies and among agencies and IGs.

- *Threat and Vulnerability Response Process*. In response to the increasing number and potential impact of threats and vulnerabilities, OMB will continue to focus on improving the federal government's incident prevention and management capabilities. Such improvements include an increased emphasis on reducing the impact of worms and viruses through more timely installation of patches for known vulnerabilities, and improved information sharing to rapidly identify and respond to cyber threats and critical vulnerabilities. OMB also notes the critical importance of agency business continuity plans to mitigating the impact of threats and vulnerabilities.

Finally, OMB's March 2004 report to the Congress identifies several other issues, and provides additional summary and agency-specific information. These include the following:

- As one of the changes or additions introduced by FISMA, a stronger emphasis is placed on configuration management. Specifically, FISMA requires each agency to develop specific system configuration requirements that meet its own needs and ensure compliance with them. According to the report, this provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Further, adequate ongoing monitoring and maintenance must accompany the establishment of such configuration requirements.

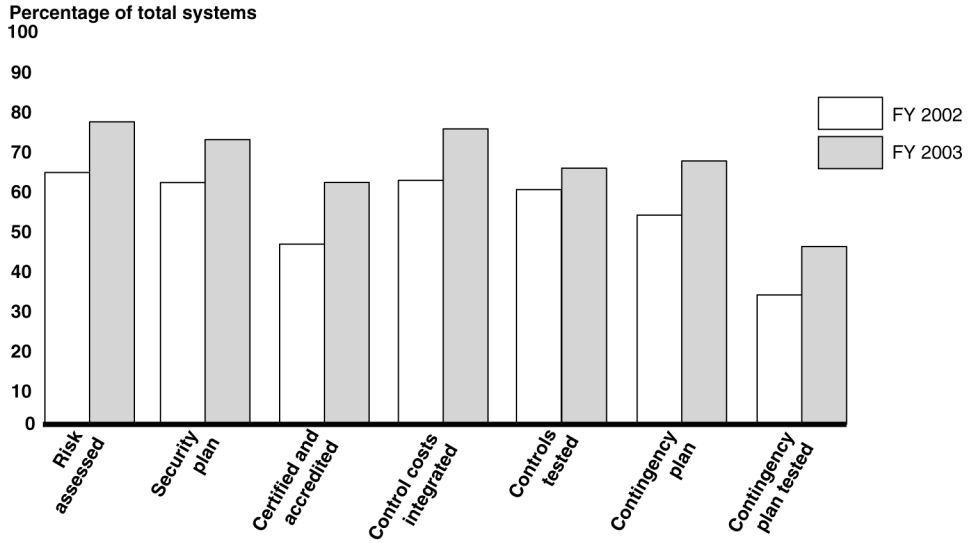
- Federal funding for IT security increased from $2.7 billion in fiscal year 2002 to $4.2 billion in fiscal year 2003. The report also continues to emphasize that, historically, a review of IT security spending and security results has demonstrated that spending is not a statistically significant factor in determining agency security performance. Rather, the key is effectively incorporating IT security in agency management actions and implementing IT security throughout the lifecycle of a system.

- The report appendixes provide an overview of the federal government's IT security program, a summary of performance by 55 small and independent agencies, and individual summaries for each of the 24 large agencies.

FISMA Reports Highlight Overall Increases in Performance Measures, But Individual Agency Results Vary Widely

Overall, fiscal year 2003 data reported by the agencies for a subset of OMB's performance measures show increasing numbers of systems meeting the requirements represented by these measures. For example, as shown in table 1, the reported percentage of systems authorized for processing following certification and accreditation increased from 47 percent for fiscal year 2002 to 62 percent for fiscal year 2003—an increase of 15 percentage points. In addition, the reported number of systems assessed for risk and assigned a level of risk increased by 13 percentage points from 65 percent for fiscal year 2002 to 78 percent for fiscal year 2003. Reported increases for other measures ranged from 4 to 15 percentage points. Figure 1 illustrates the reported overall status of the 24 agencies in meeting these requirements and the increases between fiscal years 2002 and 2003.

Figure 1: Reported Performance Measurement Data for Selected Information Security Requirements for 24 Large Federal Agencies



Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

This subset of performance measures highlights important information security requirements. However, agencies' FISMA reports also address other specific statutory requirements, regarding such elements as incident response capabilities, information security training, review of agency contractor operations and facilities, and remediation processes. The agency reports, as well as the IGs independent evaluations are intended to address all the FISMA requirements, and it is these reports and evaluations

that your subcommittee reviewed in assigning agency grades for your December 2003 computer security report card.

The data and other information submitted for fiscal year 2003 FISMA reporting did show overall increases by many agencies for certain measures, but also that wide variances existed among the agencies. As discussed earlier, we did not validate the accuracy of the data reported by the agencies, but did analyze the IGs' fiscal year 2003 FISMA reports to identify issues related to the accuracy of this information. Also as discussed later, we noted opportunities to improve the usefulness of agency-reported data. Further, in considering FISMA data, it is important to note that as more systems are subject to the certification and accreditation process and periodically tested, it is probable that additional significant weaknesses will be identified; and until all systems have contingency plans that are periodically tested, agencies have limited assurance that they will be able to recover from unexpected events. Summaries of results reported for specific requirements follow.[13]

Risk Assessment

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. OMB, through information security policy set forth in its Circular A-130,[14] also requires an assessment of risk as part of a risk-

[13]Our summarization and categorization of agency-reported information included data provided for the OMB-prescribed performance measures. In several instances, agency reports either did not address or provide sufficient data for a question or measure. IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. In addition, the DOD IG did not submit an independent evaluation report that provided the required data for fiscal year 2003.

[14]Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130, Revised, Transmittal Memorandum No. 4, Appendix III, "Security of Federal Automated Information Resources" (Nov. 28, 2000).

based approach to determining adequate, cost-effective security for a system.[15]

As defined in NIST's current draft revision of its *Risk Management Guide for Information Technology Systems*, risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level where risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.[16] Risk assessment is the first process in the risk management process, and organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its systems development life cycle. Our best practices work has also shown that risk assessments are an essential element of risk management and overall security program management, and are an integral part of the management processes of leading organizations.[17] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls.

To measure agencies' performance in implementing this requirement, OMB mandates that agencies' FISMA reports provide the number and percentage of systems that have been assessed for risk.

Reporting for this measure continued to show overall increases. Specifically, 14 of the 24 agencies reported an increase in the percentage of systems assessed for risk for fiscal year 2003 as compared with fiscal year 2002. Further, as illustrated in figure 2, 12 agencies reported that they had assessed risk for 90 to 100 percent of their systems for fiscal year 2003, and only 4 of the remaining 13 agencies reported that less than half

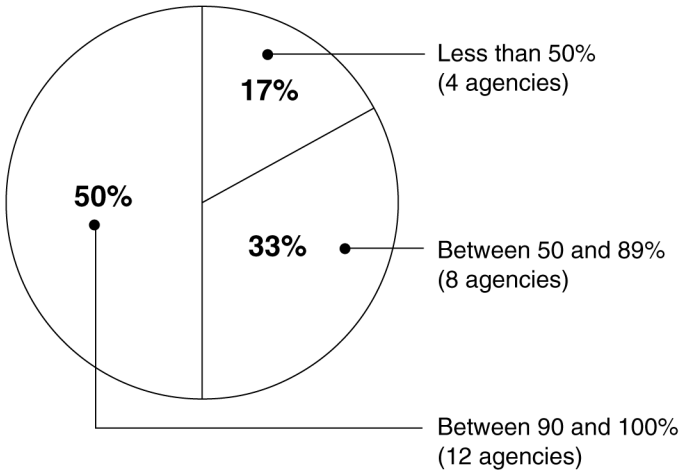
[15]OMB describes security requirements for both *general support systems* and *major applications*. A general support systems is defined as an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A major application is defined as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[16]National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Draft Special Publication 800-30 Rev A (January 2004).

[17]GAO/AIMD-98-68.

of their systems had been assessed for risk (compared with 8 agencies for fiscal year 2002).

Figure 2: Percentage of Systems Assessed for Risk for Fiscal Year 2003



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

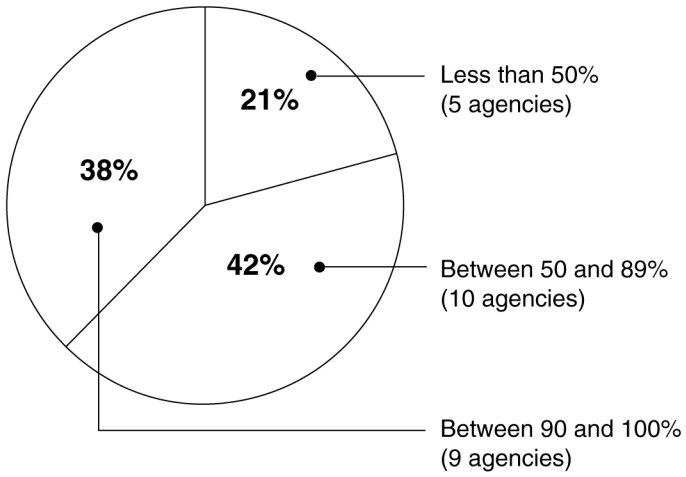
Security Plans

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. According to NIST security plan 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. OMB Circular A-130 requires that agencies prepare IT system security plans consistent with NIST guidance, and that these plans contain specific elements, including rules of behavior for system use, required training in security responsibilities, personnel controls, technical security techniques and controls, continuity of operations, incident response, and system interconnection.[18] Agencies are also to update security plans as part of the cycle for reaccrediting system processing.

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

As a performance measure for this requirement, OMB requires that agencies report number and percentage of systems with up-to-date security plans. Agency data reported for this measure showed overall increases for fiscal year 2003, with a total of 9 agencies reporting up-to-date security plans for 90 percent or more of their systems compared with 7 agencies for fiscal year 2002. Further, of the remaining 15 agencies, only 5 reported that less than 50 percent of their systems had up-to-date security plans, compared with 9 agencies in 2002. Figure 3 summarizes overall fiscal year 2003 results.

Figure 3: Percentage of Systems with Up-to-Date Security Plans for Fiscal Year 2003



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

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

Certification and Accreditation

As part of its responsibilities under FISMA, OMB is required to develop and oversee the implementation of policies, principles, standards, and guidelines on information security. 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

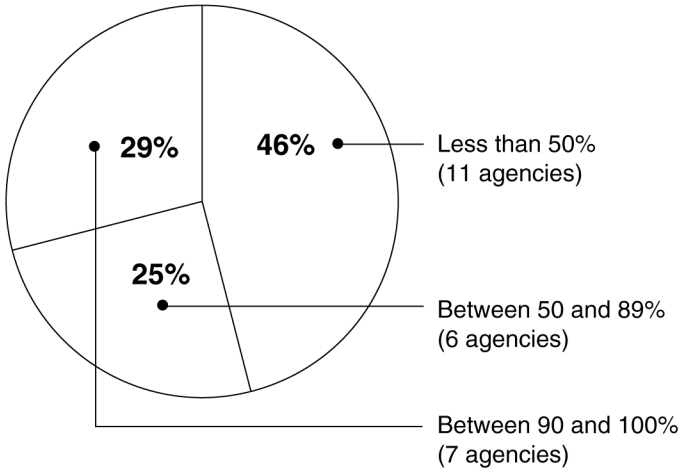
controls established in an information system's security plan. NIST is currently in the process of updating its guidance for the certification and accreditation of federal systems (except for national security systems).[19] This guidance is to be used in conjunction with other standards and guidance that FISMA requires NIST to issue—documents that, when completed, are intended to provide a structured yet flexible framework for identifying, employing, and evaluating the security controls in federal information systems.

Because OMB considers system certification and accreditation to be such an important information security quality control, for FISMA reporting, it requires agencies to report the number of systems authorized for processing after certification and accreditation.

Data reported for this measure showed overall increases for most agencies. For example, 17 agencies reported increases in the percentage of systems authorized compared with their percentages last year. In addition, 7 agencies reported that they had authorized 90 to 100 percent of their systems compared with only 3 agencies last year. However, 11 agencies reported they had authorized less than 50 percent of their systems, but this also indicated some improvement compared with the 13 agencies that reported less than 50 percent last year (which included 3 that reported none). Figure 4 summarizes overall results for the 24 agencies for fiscal year 2003.

[19]National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Second Public Draft, Special Publication 800-37 (June 2003).

Figure 4: Percentage of Systems during Fiscal Year 2003 that are Authorized for Processing after Certification and Accreditation



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

The results of the IGs' independent evaluations showed deficiencies in agencies' system certifications and accreditations, including instances in which certifications and accreditations were not were not current and controls were not tested. In addition, at the request of the House Committee on Government Reform and your subcommittee, we are currently reviewing federal agencies' certification and accreditation processes. Preliminary results of our work indicate that the majority of the 24 large agencies reported that they are using NIST or other prescribed guidance for their system certifications and accreditations. However, our reviews of the certification and accreditation of selected systems at selected agencies identified instances where documentation did not show that specific criteria were 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. Unless agencies ensure that their certifications and accreditations meet appropriate criteria, the value of this process as a management control for ensuring information system security is limited, and agency reported performance data may not accurately reflect the status of an agency's efforts to implement this requirement.

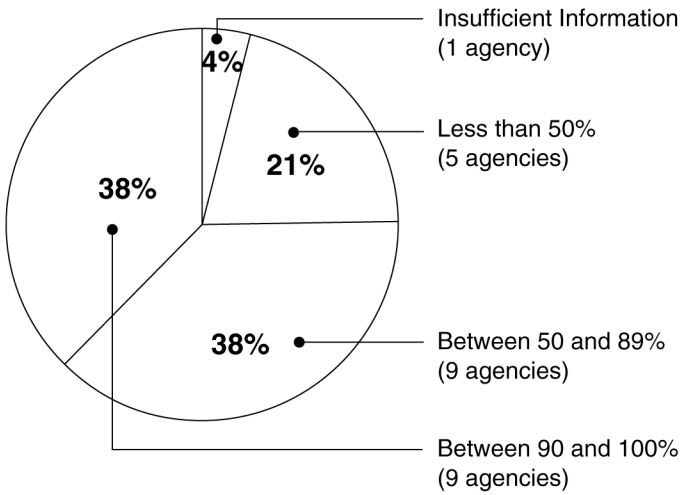
Integration of Security Costs into the System Life Cycle

OMB requires that agencies' budget submissions specifically identify security costs as part of life-cycle costs for their IT investments and has provided criteria to be considered in determining such costs.[20] OMB also provided these security cost criteria in its FISMA guidance and required agencies to report their IT security spending, including those critical infrastructure protection costs that apply to the protection of government operations and assets. Among other questions related to including security costs in IT investments, OMB requires that the agencies report the number of systems that have security control costs integrated into their system life cycles.

Fiscal year 2003 reporting for this measure showed that agencies are increasingly integrating security control costs into the life cycle of their systems. Specifically, 15 agencies reported increases in the number of systems integrating security costs, compared with the number reported last year. Also, as shown in figure 5, 9 agencies reported meeting this measure for 90 to 100 percent of their systems.

[20]Criteria to be considered include the products, procedures, and personnel (federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Examples include costs for risk assessment; security planning and policies; certification and accreditation; specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security); authentication or cryptographic applications; education, awareness, and training; system reviews/evaluations (including security control testing and evaluation); oversight or compliance inspections; development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment; contingency planning and testing; physical and environmental controls for hardware and software; auditing and monitoring; computer security investigations and forensics; and reviews, inspections, audits and other evaluations performed on contractor facilities and operations. Agencies must also include the products, procedures, and personnel that have as an incidental or integral component a quantifiable benefit to IT security for the specific IT investment, such as configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; and systems administrator functions. For the security costs of application investments, agencies should also appropriately allocate the costs of networks, which may provide some or all of the necessary security controls for the associated applications.

Figure 5: Percentage of Systems that Have Security Control Costs Integrated into the Life Cycle of their Systems for Fiscal Year 2003



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

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

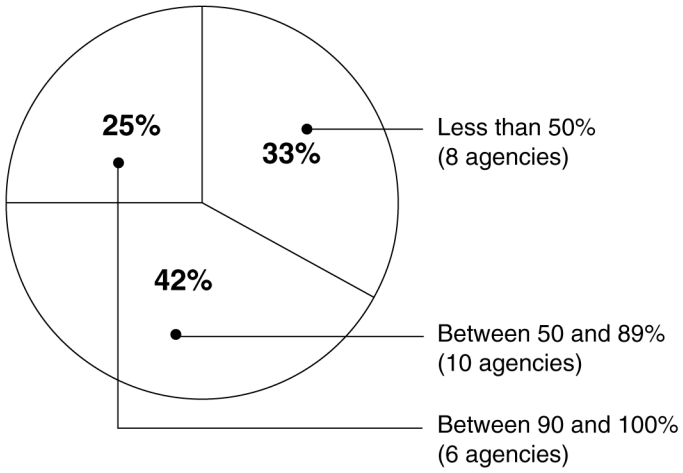
Security Control Testing and Evaluation

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 our audits to help provide a more complete picture of the agencies' security postures.

As a performance measure for this requirement, OMB mandates that agencies report the number of systems for which security controls have been tested and evaluated. Fiscal year 2003 data reported for this measure

showed that a total of 15 agencies reported an increase in the overall percentage of systems being tested and evaluated. However, 8 agencies still reported that they had tested the controls of less than 50 percent of their systems (compared with 10 agencies last year) and only 6 of the remaining 16 agencies reported testing and evaluating the controls for 90 percent or more of their systems (compared with 4 agencies last year). Figure 6 shows the overall results for fiscal year 2003.

Figure 6: Percentage of Systems with Security Controls Tested during Fiscal Year 2003



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

Contingency Plans

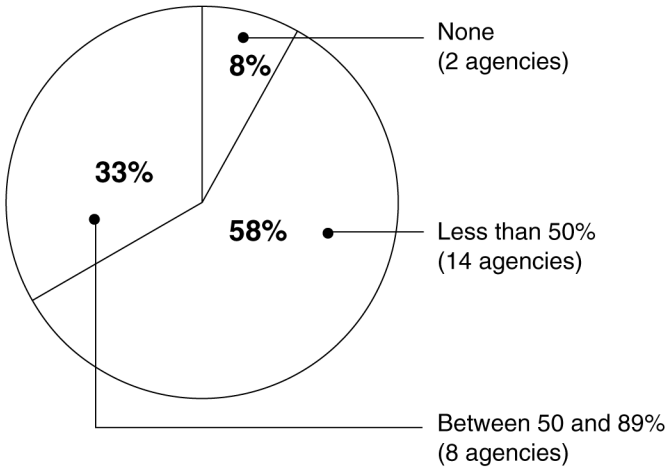
FISMA requires that agencies' information security programs include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities, in case usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, accidental loss of files, or major disaster. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations.

The testing of contingency plans is essential to determine whether they 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 mandates that agencies report the number of systems that have a contingency plan and the number with contingency plans that have been tested. Agencies' reported fiscal year 2003 data for these measures showed that contingency planning remains a problem area for many agencies. Specifically, a total of 11 agencies report that less than half of their systems have contingency plans and of the remaining 13 agencies, only 6 have contingency plans for 90 to 100 percent of their systems. In addition, a total of 14 agencies reported that they had tested contingency plans for less than half of their systems, including 2 agencies that reported testing none. Figure 7 provides overall results for fiscal year 2003 contingency plan testing.

Figure 7: Percentage of Systems with Contingency Plans That Have Been Tested for Fiscal Year 2003



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

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

Security Training

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems

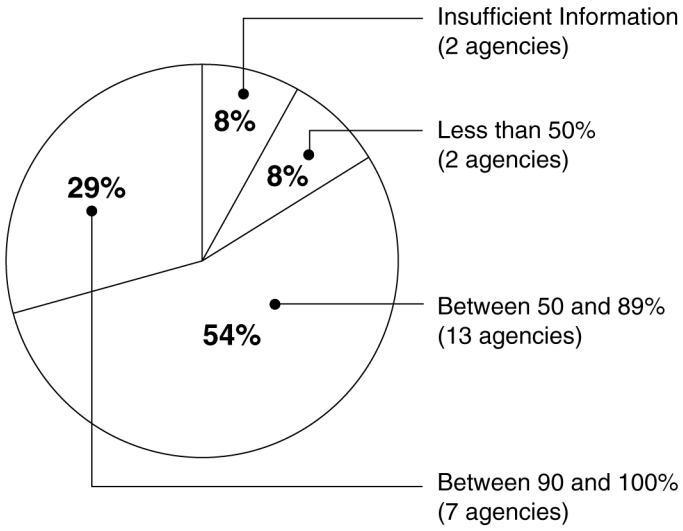
that support the operations and assets of the agency, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide training on information security to personnel with significant security responsibilities. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools.

As performance measures for FISMA training requirements, OMB has the agencies report the number of employees who received IT security training during fiscal year 2003 and the number of employees with significant security responsibilities who received specialized training.

Reported fiscal year 2003 data showed that 13 agencies reported that they provided security training to 90 to 100 percent of their employees and contractors compared with 9 agencies for fiscal year 2002. Of the remaining 11 agencies, only 3 reported that such training was provided for less than half of their employees/contractors, and 1 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, reported data showed increases since fiscal year 2002. For example, a total of 7 agencies reported training for 90 to 100 percent of their employees with significant security responsibilities (compared with 5 agencies last year), and of the remaining 17 agencies, only 2 reported providing training to less than half of such employees (compared with 10 for fiscal year 2002). Figure 8 provides overall results for fiscal year 2003.

Figure 8: Percentage of Employees with Significant Security Responsibilities Receiving Specialized Training during Fiscal Year 2003



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

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

Incident Handling

Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect them before significant damage can be done. 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 FISMA-required federal information security incident center and other entities, as appropriate, including law enforcement agencies and relevant IGs. OMB information security policy has also required that system security plans ensure a capability to provide help to users when a security incident occurs in the

system and to share information concerning common vulnerabilities and threats. In addition, NIST has provided guidance to assist organizations in establishing computer security incident-response capabilities and in handling incidents efficiently and effectively.[21]

OMB requires agencies to report several performance measures and other information for FISMA related to detecting, reporting, and responding to security incidents. These include the number of agency components with an incident handling and response capability, whether the agency and its major components share incident information with the Federal Computer Incident Response Center (FedCIRC)[22] in a timely manner, and the numbers of incidents reported. OMB also requires that agencies report on how they confirm that patches[23] have been tested and installed in a timely manner and whether they are a member of FedCIRC's Patch Authentication and Distribution Capability, which provides agencies with information on trusted, authenticated patches for their specific technologies without charge.[24]

Agency-reported data showed that many agencies have established and implemented incident-response capabilities for their components. For example, 17 agencies reported that for fiscal year 2003, 90 percent or more of their components had incident handling and response capabilities (compared to 12 agencies for fiscal year 2002). Also, a total of 18 agencies reported that their components report incidents to FedCIRC either themselves or centrally through one group.

A total of 22 agencies reported that they confirm patches have been tested and installed in a timely manner. In contrast, of the 23 IGs that reported,

[21]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 (January 2004).

[22]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention, and recognition for the federal government.

[23]A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered. Patch management is the process of effectively applying available patches.

[24]According to a DHS official, the department recently decided to terminate the Patch Authentication and Distribution Capability based on low levels of usage, negative agency feedback on its usefulness, and the cost to make significant upgrades. Further, many of its customers only used this service for patch notification, which can generally be obtained through vendors at no cost.

11 responded that the agency confirmed that patches have been tested and installed in a timely manner; 5 that the agency did but not consistently; and 6 that the agency did not (1 other IG did not provide sufficient data). A total of 19 agencies also reported that they were a member of FedCIRC's Patch Authentication and Distribution Capability.

In our September 2003 testimony, we discussed the criticality of the patch management process in helping to alleviate many of the challenges involved in securing computing systems from attack.[25] We also identified common practices for effective patch management found in security-related literature from several groups, including NIST, Microsoft,[26] patch management software vendors, and other computer-security experts. These practices included

- senior executive support of the process;
- standardized patch management policies, procedures, and tools;
- dedicated resources and clearly assigned responsibilities for ensuring that the patch management process is effective;
- current inventory of all hardware equipment, software packages, services, and other technologies installed and used by the organization;
- proactive identification of relevant vulnerabilities and patches;
- assessment of the risk of applying the patch considering the importance of the system to operations, the criticality of the vulnerability, and the likelihood that the patch will disrupt the system;
- testing each individual patch against various systems configurations in a test environment before installing it enterprisewide to determine any impact on the network;
- effective patch distribution to all users; and

[25]U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Sep. 10, 2003).

[26]Microsoft Corporation, *Solutions for Security, Solutions for Management: The Microsoft Guide to Security Patch Management* (Redmond, WA: 2003).

- regular monitoring through network and host vulnerability scanning to assess whether patches have been effectively applied.

In addition to these practices, we identified several steps to be considered when addressing software vulnerabilities, including:

- deploying other technologies, such as antivirus software, firewalls, and other network security tools, to provide additional defenses against attacks;
- employing more rigorous engineering practices in designing, implementing, and testing software products to reduce the number of potential vulnerabilities;
- improving tools to more effectively and efficiently manage patching;
- researching and developing technologies to prevent, detect, and recover from attacks as well as to identify their perpetrators, such as more sophisticated firewalls to keep serious attackers out, better intrusion-detection systems that can distinguish serious attacks from nuisance probes and scans, systems that can isolate compromised areas and reconfigure while continuing to operate, and techniques to identify individuals responsible for specific incidents; and
- ensuring effective, tested contingency planning processes and procedures.

Security of Contractor-Provided Services

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.

As a performance measure for the security of contractor-provided security, OMB had the agencies report the number of contractor facilities

or operations reviewed and to respond as to whether or not they used appropriate methods (such as audits or inspections and agreed-upon IT security requirements) to ensure that contractor-provided services for their programs and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

Fiscal year 2003 data reported for these measures showed that 10 of the 24 agencies reported that they had reviewed 90 to 100 percent of their contractor operations or facilities. Only 2 agencies reported having reviewed less than half of their contractor operations or facilities, and two others provided insufficient data for this measure. In addition, 22 agencies reported that they used appropriate methods to ensure that contractor-provided services are adequately secure and meet the requirements of FISMA. Of the remaining two agencies, one reported that it did not use appropriate methods and one reported partial compliance. Although these reported results indicate overall increases from fiscal year 2002, the IGs' evaluations provided different results. For example, although the IG evaluations did not always address these measures, 9 of the 15 IGs that did report showed that less than half of contractor operations or facilities were reviewed. Further, only 12 IGs reported that the agency used appropriate methods to ensure that contractor-provided services are adequately secure and meet the requirements of FISMA, while 7 reported that their agencies did not.

Plan of Action and Milestones

FISMA requires that agencies' information security programs include 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. Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. Further, a centralized process for monitoring and managing remedial actions enables the agency to identify trends, root causes, and entitywide solutions.

As discussed previously, as part of GISRA implementation, OMB began requiring that agencies report on the status of their remediation efforts through POA&Ms and quarterly updates. In addition, for fiscal year 2003 FISMA reporting, OMB had agency IGs assess whether the agency had developed, implemented, and was managing an agencywide plan of action and milestone process according to specific criteria, such as whether agency program officials and the CIO develop, implement, and manage POA&Ms for every system that they own and operate (systems that

support their programs) that has an IT security weakness; and whether the agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.

Overall, the IGs' responses to these criteria showed that many agencies still do not use the POA&M process to manage the correction of their information security weaknesses. For example, as part of monitoring the status corrective actions, 20 of the 23 IGs that reported responded that the agency CIO tracked POA&M data centrally on at least a quarterly basis, but only 12 reported that the CIO maintained POA&Ms for every system that has an IT weakness. Further, 14 IGs reported that their agency POA&M process did not prioritize IT security weaknesses to ensure that significant weaknesses are addressed in a timely manner and receive appropriate resources. Reported IG responses to these and other criteria are summarized in table 2.

Table 2: Summary of Inspector General Assessment of Agency POA&M Processes

	Inspector General Responses					
	Yes		No		Data not provided	
OMB reporting criteria	Number	(%)	Number	(%)	Number	(%)
Agency program officials have POA&Ms for every system they own and operate that has an IT security weakness	11	(48)	10	(43)	2	(9)
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress	14	(61)	8	(35)	1	(4)
Agency CIO has POA&Ms for every system it owns and operates that has an IT security weakness	12	(52)	10	(44)[a]	1	(4)
Agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis	20	(87)	3	(13)	0	(0)
POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses	14	(61)	8	(35)	1	(4)
System-level POA&Ms are tied directly to the system budget request through the IT business case to tie the justification for IT security funds to the budget process	10	(44)[a]	12	(52)	1	(4)
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms	18	(78)	5	(22)	0	(0)
The agency's POA&M process represents a prioritization of agency IT security weaknesses to ensure that significant weaknesses are addressed in a timely manner and receive appropriate resources	8	(35)	14	(61)	1	(4)

Source: Agency Fiscal Year 2003 FISMA reports and GAO (analysis).

[a]Rounded up to total 100 percent.

Opportunities Exist to Improve the Usefulness of Performance Measurement Data

Periodic reporting of performance measures tied to FISMA requirements and related analysis can provide valuable information on the status and progress of agency efforts to implement effective security management programs, thereby assisting agency management, OMB and the Congress in their management and oversight roles. However, several opportunities exist to improve the usefulness of such information as indicators of both governmentwide and agency-specific performance in implementing information security requirements. As discussed earlier, OMB plans to further emphasize performance measurement in next year's FISMA reporting guidance, including evolving measures to identify the quality of work performed, targeting IG efforts to assess key security processes, and clarifying certain definitions. In developing its guidance, OMB can

consider how their efforts can help to address the following factors that lessen the usefulness of current performance measurement data:

- *Limited assurance of data reliability and quality*. The performance measures reported by the agencies are primarily based on self-assessments and are not independently validated. OMB did not require the IGs to validate agency responses to the performance measures, but did instruct them to assess the reliability of the data for the subset of systems they evaluate as part of their independent evaluations. Although not consistently addressed by all the IGs, some IG evaluations did identify problems with data reliability and quality that could affect agency performance data. For example, for the performance measure on the number of agency systems authorized for processing after certification and accreditation, 6 IGs indicated different results than those reported by their agencies for reasons such as out-of-date certifications and accreditations (systems are to be reaccredited at least every 3 years). Further, other IGs identified problems with the quality of the certifications and accreditations, such as security control reviews not being performed.

- *Accuracy of agency system 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. As mentioned, FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. However, according to their fiscal year 2003 FISMA reports, only 13 of the 24 agencies reported that they had completed their system inventories. Further, independent evaluations by IGs for 3 of these 13 agencies did not agree that system inventories were complete. In addition, although there was little change in the reported total number of systems shown for the 24 agencies (an increase of only 41 systems from 7,957 systems for fiscal year 2002 to 7,998 systems for fiscal year 2003, large changes in individual agencies' total systems from year to year could make it more difficult to interpret changes in their performance measure results. For example, the total number of systems reported by the Department of Agriculture decreased by 55 percent from 605 for fiscal year 2002 to 271 for fiscal year 2003, which the department attributed, in large part, to its efforts to develop the FISMA-required inventory of major information systems. At the same time, all of the department's key performance measures increased, with some, such as systems assessed for risk,

showing a large increase (from 18 percent for fiscal year 2002 to 72 percent for fiscal year 2003).

- *Limited Department of Defense data*. In interpreting overall results for the federal government, it is important to note that reported numbers include only a small sample of the thousands of systems identified by DOD. Attributing its size and complexity and the considerable lead time necessary to allow for the collection of specific metrics and the approval process by each service and agency, DOD determined that the collection of a sample of system and network performance metrics would effectively support its emphasis on network-centric operations and complement its overall information assurance security reporting. Obtaining OMB concurrence with this approach, DOD provided performance measurement data on a sample of 378 systems in its fiscal year 2003 FISMA report. As OMB reported in its fiscal year 2003 report to the Congress, DOD reported a total of 3,557 systems for the department—almost half of the combined total systems for the other 23 agencies. OMB also reported that DOD plans to report on all systems for the fiscal year 2004 reporting cycle. As a result, including performance data on all DOD systems for fiscal year 2004 could significantly affect the overall performance measurement results both for DOD and governmentwide.

- *Data reported in aggregate, not according to system risk*. Performance measurement data are reported on the total number of agency systems and do not indicate the relative importance or risk of the systems for which FISMA requirements have been met. 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 2003 show that 48 percent of the total number of systems have tested contingency plans, but do not indicate to what extent these 48 percent include the agencies' most important systems. Therefore, agencies, the administration, and the Congress cannot be sure that critical federal operations can be restored if an unexpected event disrupts service. As required by FISMA, NIST recently issued its *Standards for Security Categorization of Federal Information and Information Systems* to provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs and consistent reporting to OMB and the Congress on the adequacy and effectiveness of information security

policies, procedures, and practices.[27] These standards, which are discussed later in greater detail, would require agencies to categorize their information systems according to three levels of potential impact on organizations or individuals—high, moderate, and low—should there be a breach of security.

- *Refinement of performance measures to improve quality of analysis.* Refinement of performance measures can provide more useful information about the quality of agency processes. For example, as discussed earlier, GAO and the IGs have noted issues concerning the quality of the certification and accreditation process. Additional information reported on key aspects of certification and accreditation would provide better information to assess whether they were performed consistently. As also discussed earlier, OMB's fiscal year 2003 FISMA report to the Congress also identified the need to evolve performance measures to provide better quality information.

Status of NIST Efforts

Since FISMA was enacted in December 2002, NIST has taken a number of actions to develop required security-related standards and guidance. These actions include the following:

- In December 2003 it issued the final version of its *Standards for Security Categorization of Federal Information and Information Systems* (FIPS Publication 199). NIST was required to submit these categorization standards to the Secretary of Commerce for promulgation no later than 12 months after FISMA was enacted. The standards establish 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). These standards are intended to provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs, and consistent reporting to OMB and the Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

- Also in December 2003, it issued the initial public draft of its *Guide for Mapping Types of Information and Information Systems to Security Categories* (Special Publication 800-60). Required to be issued 18 months

[27]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.

after FISMA enactment, this guidance is to assist agencies in categorizing information and information systems according to impact levels for confidentiality, integrity, and availability as provided in NIST's security categorization standards (FIPS Publication 199).

- In October 2003 it issued an initial public draft of *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) to provide guidelines for selecting and specifying security controls for information systems categorized in accordance with FIPS Publication 199. This draft includes baseline security controls for low and moderate impact information systems, with controls for high impact systems to be provided in subsequent drafts. This publication, when completed, will serve as interim guidance until 2005 (36 months after FISMA enactment), which is the statutory deadline to publish minimum standards for all non-national-security systems. In addition, testing and evaluation procedures used to verify the effectiveness of security controls are to be provided this spring in NIST's Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems (Special Publication 800-53A).

- In August 2003 it issued *Guideline for Identifying an Information System as a National Security System* (Special Publication 800-59). This document provides guidelines developed in conjunction with DOD, including the National Security Agency, to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements. Except for national security systems identified by FISMA, the Secretary of Commerce is responsible for prescribing standards and guidelines developed by NIST. DOD and the Director of Central Intelligence have authority to develop policies, guidelines, and standards for national security systems. The Director is also responsible for policies relating to systems processing intelligence information.

According to a NIST official, the agency has also made progress in implementing other FISMA requirements. For example, it is continuing to provide consultative services to agencies on FISMA related information security issues and has established a federal agencies security practices Web site 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 underway within the federal government.

FISMA also requires NIST to prepare an annual public report on activities undertaken in the previous year and planned for the coming year, to carry out its responsibilities. According to a NIST official, this report should be issued this month.

In addition to its responsibilities under FISMA, NIST has issued or is developing other information security guidance that supports this law. Along with its guidance on incident handling, building an information security awareness program, and draft guidance on both certification and accreditation and risk management, NIST has also issued *Security Metrics Guide for Information Technology Systems*[28] and *Security Considerations in the Information System Development Life Cycle: Recommendations of the National Institute of Standards and Technology*. [29]

Current budget constraints may, however, affect NIST's future work. FISMA established new responsibilities for this agency and authorized an appropriation of $20 million for each fiscal year, 2003 through 2007. However, according to NIST, funding for the Computer Security Division, the organization responsible for FISMA activities, was reduced from last year, and this will affect this division's information security and critical infrastructure protection work.

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

- operating a computer security expert assist team (CSEAT) to assist federal agencies in identifying and resolving IT security problems;
- conducting security research in areas such as access control, wireless, mobile agents, smart-cards, and quantum computing;
- improving the security of control systems that manage key elements of the country's critical infrastructure; and

[28]National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55 (July 2003).

[29]National Institute of Standards and Technology, *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64 (October 2003).

- performing cyber security product certifications required for government procurements.

The Cyber Security Research and Development Act also assigned information security responsibilities to NIST and authorized funding. These responsibilities include

- providing research grants to institutions of higher education or other research institutions to support short-term research aimed at improving the security of computer systems; growth of emerging technologies associated with the security of networked systems; strategies to improve the security of real-time computing and communications systems for use in process control; and multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.

- developing cyber security checklists (and establishing priorities for their development) that set forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the federal government.

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 apparent progress shown by increases in key performance measures, most agencies still have not reached the level of performance that demonstrates that they have implemented the agencywide information security program mandated by FISMA. If information security is to continue to improve, agency management must remain committed to these efforts and establish management processes that ensure that requirements are implemented for all their major systems, including new requirements to categorize their systems and incorporate mandatory minimum security controls. Performance measures will continue to be a key tool to both hold agencies accountable and provide a barometer of the overall status of federal information security. For this reason, it is increasingly important that agencies' monitoring, review, and evaluation processes provide the Congress, the administration, and agency management with assurance that these measures accurately reflect agency progress. Opportunities to provide this assurance and improve the usefulness of agencies' performance measurement data include IG validation of reported data,

categorization of the data according to system risk levels, and refinement of the measures to provide more information about the quality of agency processes.

Achieving significant and sustainable results will likely require agencies to develop programs and processes that prioritize and routinely monitor and manage their information security efforts. Further, agencies will need to ensure that systems and processes are in place to provide information and facilitate the day-to-day management of information security throughout the agency, as well as to verify the reliability of reported performance information.

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

If you should have any questions about this testimony, please contact me at (202) 512-3317 or Ben Ritt, Assistant Director, at (202) 512-6443. We can also be reached by e-mail at daceyr@gao.gov and rittw@gao.gov, respectively.

Other individuals making key contributions to this testimony included Larry Crosland, Mark Fostek, Danielle Hollomon, and Barbarol James.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548