

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 10 a.m. EDT
Tuesday, June 24, 2003

INFORMATION SECURITY

Continued Efforts Needed to Fully Implement Statutory Requirements

Statement of Robert F. Dacey
Director, Information Security Issues



GAO

Accountability * Integrity * Reliability

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



INFORMATION SECURITY

Continued Efforts Needed to Fully Implement Statutory Requirements

Highlights of [GAO-03-852T](#), testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

Why GAO Did This Study

Since 1996, GAO has reported that poor information security in the federal government is a widespread problem with potentially devastating consequences. Further, GAO has identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003. To strengthen information security practices throughout the federal government, information security legislation has been enacted.

This testimony discusses efforts by federal departments and the administration to implement information security requirements mandated by law. In so doing, it examines

- overall information security weaknesses and challenges that the government faces, and the status of actions to address them, as reported by the Office of Management and Budget (OMB);
- GAO’s evaluation of agency efforts to implement federal information security requirements and correct identified weaknesses; and
- new requirements mandated by the Federal Information Security Management Act of 2002 (FISMA).

www.gao.gov/cgi-bin/getrpt?GAO-03-852T.

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 daceyrf@gao.gov.

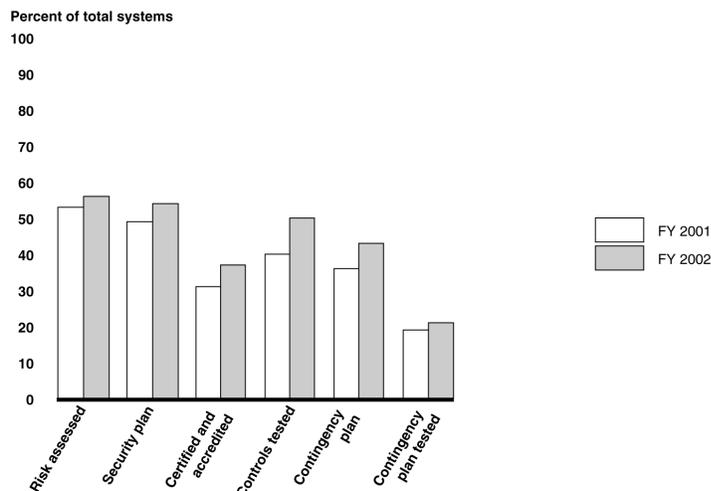
What GAO Found

Based on the fiscal year 2002 reports submitted to OMB, the federal government has made limited overall progress in implementing statutory information security requirements, although a number of benefits have resulted. Among these benefits are several actions taken and planned to address governmentwide information security weaknesses and challenges, such as lack of senior management attention. Nevertheless, as indicated by selected quantitative performance measures for the largest federal agencies, progress has been limited. Specifically, excluding data for one agency that were not comparable for fiscal years 2001 and 2002, improvements for 23 agencies ranged from 3 to 10 percentage points for the selected measures (see figure).

GAO’s analyses of agencies’ reports and evaluations confirmed that many agencies have not implemented security requirements for most of their systems, such as performing risk assessments and testing controls. Further, the usefulness of agency corrective action plans may be limited when they do not identify all weaknesses or contain realistic completion dates. Agencies also continue to face challenges in effectively implementing and managing their overall information security programs.

FISMA provisions establish additional requirements that, among other things, can assist agencies in implementing effective information security programs. However, attaining significant and sustainable results in implementing such requirements will also likely require processes that prioritize and routinely monitor and manage agency efforts, as well as continued congressional and administration oversight.

Performance Measure Percentages for Selected Information Security Requirements^a



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform and GAO (analysis).

^aExcludes National Aeronautics and Space Administration data.

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 statutory information security requirements. Since 1996,¹ we have reported that poor information security in the federal government is a widespread problem with potentially devastating consequences. Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.² 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 Government Information Security Reform provisions (commonly known as GISRA) to strengthen information security practices throughout the federal government.³ GISRA established information security program, evaluation, and reporting requirements for federal agencies, which are now permanently authorized and strengthened through the recently enacted Federal Information Security Management Act of 2002 (FISMA).⁴

In my testimony today, I will first summarize the federal government's overall information security weaknesses and challenges, as well as the status of the administration's efforts to address them as discussed in the May 2003 Office of Management and Budget (OMB) report to the Congress on fiscal year 2002 GISRA implementation.⁵ I will also discuss the results of our evaluation of efforts by OMB and 24 of the largest federal agencies to implement federal information security requirements and correct identified weaknesses. Finally, I will describe new information security requirements contained in FISMA that can assist agencies in implementing effective information security.

In conducting this review, we analyzed OMB's May 2003 report to the Congress on GISRA implementation. We also compared the results of OMB's report with the results of our analyses of fiscal year 2002 GISRA reporting by 24 of the largest federal agencies and their inspectors general (IGs), which we had previously

¹U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

²U.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).

³*Government Information Security Reform, Title X, Subtitle G, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L.106-398, October 30, 2000.

⁴*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.

⁵Office of Management and Budget, *FY 2002 Report to Congress on Federal Government Information Security Reform*, May 16, 2003.

reported in testimony before your subcommittee in April 2003.⁶ We did not validate the accuracy of the data reported by OMB or by the agencies. We also analyzed the provisions of FISMA. We performed our work in June 2003, in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2002 report to the Congress, OMB reported that the federal government had made significant strides in addressing serious and pervasive information technology (IT) security problems, but that much work remained. It highlighted actions and progress to address previously identified governmentwide weaknesses, such as lack of senior management attention to information security, as well as planned actions to address newly-reported challenges, such as agencies continuing to identify the same security weaknesses year after year. OMB also reported significant progress in agencies' IT security performance as indicated by the quantitative performance measures that OMB required agencies to report beginning in fiscal year 2002. These measures include the number of systems that have been assessed for risk, have an up-to-date security plan, and for which security controls have been tested. In particular, for selected performance measures for 24 large federal agencies, OMB's report showed increases from fiscal year 2001 to fiscal year 2002 ranging from 18 to 27 percentage points.

Although our review of GISRA implementation also showed a number of benefits resulting from this legislation, our analyses of governmentwide performance measures showed more limited overall progress. Excluding one of the 24 agencies because its performance data for these fiscal years was not comparable, our analyses showed that increases for these measures ranged from only 3 to 10 percentage points. Further, our analyses of individual agency reports showed that significant challenges remained in implementing information security requirements. For example, of the 24 agencies, 11 reported that they had assessed risk for 90 to 100 percent of their systems for fiscal year 2002, but 8 reported that they had assessed risk for less than 50 percent of their systems.

Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. However, our analyses of agencies' OMB-required corrective action plans for fiscal year 2002, IGs' evaluations of these plans, and available quarterly updates showed that plan usefulness could be limited when plans do not identify all weaknesses, provide realistic completion estimates, or prioritize actions. For example, of 14 agency IGs

⁶U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-546T (Washington, D.C.: Apr. 8, 2003).

who reported whether their agency's corrective action plan addressed all identified significant weaknesses, 5 reported that their agency's plan did and 9 reported that it did not.

The governmentwide weaknesses identified by OMB, as well as the limited progress in implementing key information security requirements, continue to emphasize that, overall, agencies are not effectively implementing and managing their information security programs. For several years we have reported that most agencies have significant weaknesses in security program management and pointed out that agencies should implement a cycle of risk management activities—activities that are now required by law. Although agency reporting provides performance information, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as to ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security.

FISMA provisions establish additional requirements that can assist the agencies in implementing effective information security programs, help ensure that agency systems incorporate appropriate controls, and provide information for administration and congressional oversight. These requirements include the designation of and establishment of specific responsibilities for an agency senior information security officer, implementation of minimum information security requirements for agency information and information systems, and required agency reporting to the Congress.

In addition to continued congressional and administration oversight, we believe that achieving significant and sustainable results, including the implementation of new requirements, will require agencies to integrate the use of techniques, such as corrective action plans and performance measures, into overall security management programs and processes that prioritize and routinely monitor and manage their information security efforts. Development of management strategies that identify specific actions, time frames, and required resources may also help to significantly improve performance.

Background

On October 30, 2000, the Congress enacted GISRA, which 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 OMB⁷ and NIST,⁸ as well as audit and best practice guidance issued by us.⁹

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. GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. OMB released its fiscal year 2001 report in February 2002¹⁰ and its fiscal year 2002 report in May 2003.

GISRA required each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program was to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;

⁷Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

⁸Numerous 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.

⁹U.S. General Accounting Office, *Federal Information System Controls 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).

¹⁰Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform*. February 2002.

-
- a process for identifying and remediating any significant deficiencies;
 - procedures for detecting, reporting, and responding to security incidents; and
 - an annual program review by agency program officials.

In addition to the responsibilities listed above, GISRA required each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems were to be performed by the agency IG or an independent evaluator, and the results of these evaluations were to be reported to OMB. For the evaluation of national security systems, special provisions included having national security agencies designate evaluators, restricting the reporting of evaluation results, and having the IG or an independent evaluator perform an audit of the independent evaluation. For national security systems, only the results of each audit of an evaluation were to be reported to OMB.

For first-year GISRA implementation, OMB provided guidance to the agencies in January 2001, and in June issued final instructions on reporting results of annual agency security program reviews and inspector general independent evaluations to OMB to provide a basis for its annual report to the Congress.¹¹ These instructions listed specific topics that the agencies were to address in their reporting, many of which were referenced back to corresponding GISRA requirements. Agencies were to report their results to OMB in September 2001—the same time they were to submit their fiscal year 2003 budget materials. In October 2001, OMB also issued detailed guidance to the agencies on reporting their strategies for correcting the security weaknesses identified through their reviews, evaluations, and other reviews or audits performed throughout the reporting period.¹² This information was to include a “plan of action and milestones” (corrective action plan) that, among other things, listed the weaknesses; showed required resources, milestones, and completion dates; and described how the agency planned to address those weaknesses. The guidance also required agencies to submit quarterly status updates of their corrective action plans to OMB. Corrective action plans were due to OMB by the end of October, and the first quarterly updates were due January 31, 2002.

¹¹Office of Management and Budget, “Guidance on Implementing the Government Information Security Reform Act,” Memorandum for the Heads of Executive Departments and Agencies, Jack Lew, Director, M-01-08, January 16, 2001; “Reporting Instructions for the Government Information Security Reform Act,” Memorandum for the Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., Director, M-01-24, June 22, 2001.

¹²Office of Management and Budget, “Guidance for Preparing and Submitting Security Plans of Action and Milestones,” Memorandum for the Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., Director, M-02-01, October 17, 2001.

For fiscal year 2002, OMB provided the agencies with updated reporting instructions and guidance on preparing and submitting corrective action plans.¹³ Agencies were again to report their GISRA review and evaluation results to OMB in September with corrective action plans due October 1, 2002, and the next quarterly update due on January 1, 2003. Although similar to its previous guidance, in response to agency requests and recommendations we made to OMB as a result of our review of fiscal year 2001 GISRA implementation,¹⁴ this guidance also incorporated several significant changes to help improve the consistency and quality of information being reported for oversight by OMB and the Congress. These changes included the following:

- Reporting instructions provided new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance. These included, for example, the number and percentage of systems assessed for risk, the number and percentage of systems certified and accredited,¹⁵ the number of contractor operations or facilities reviewed, and the number of employees with significant security responsibilities that received specialized training.
- OMB confirmed that agencies were expected to review all systems annually. It explained that GISRA requires senior agency program officials to review each security program for effectiveness at least annually, and that the purpose of the security programs discussed in GISRA is to ensure the protection of the systems and data covered by the program. Thus, a review of each system is essential to determine the program's effectiveness, and only the depth and breadth of such system reviews are flexible.
- Agencies were generally required to use all elements of NIST's *Security Self-Assessment Guide for Information Technology Systems* to review their systems unless an agency and its IG confirmed that any agency-developed methodology

¹³Office of Management and Budget, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," Memorandum for Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., M-02-09, July 2, 2002.

¹⁴U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-407 (Washington, D.C.: May 2, 2002).

¹⁵*Accreditation* is the authorization of an IT system to process, store, or transmit information, granted by a management official 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. *Certification* is the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Certification 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. 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.

captured all elements of the guide.¹⁶ The guide uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured.

- OMB requested that IGs verify that agency corrective action plans identify all known security weaknesses within an agency, including components, and are used by the IG and the agency, major components, and program officials within them, as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.
- OMB authorized agencies to release certain information from their corrective action plans 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.

OMB Reports Significant Progress and Actions to Address Governmentwide Weaknesses

In its fiscal year 2002 report to the Congress, OMB stated that the federal government had made significant strides in addressing serious and pervasive IT security problems, but that more needed to be done, particularly to address both the governmentwide weaknesses identified in its fiscal year 2001 report to the Congress and new challenges. Also, as discussed in a later section, OMB reported significant progress in agencies' IT security performance, primarily as indicated by the quantitative governmentwide performance measures that OMB required agencies to disclose beginning with their fiscal year 2002 reports.

OMB previously reported six common security weaknesses for the federal government. Actions and progress for these weaknesses reported by OMB in its fiscal year 2002 report were as follows:

Lack of senior management attention to information security. OMB reports that based on agencies' security reviews, remediation efforts, and IT budget materials, it either conditionally approves or disapproves agency security programs, and the OMB Director communicates this decision directly to each agency head. Further, OMB used the President's Management Agenda Scorecard to focus attention on

¹⁶National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001.

serious IT security weaknesses and, along with senior agency officials, to monitor agency progress on a quarterly basis. As a result, OMB concluded that senior executives at most agencies are paying greater attention to IT security.

Inadequate accountability for job and program performance related to IT security. OMB's instructions to federal agencies for fiscal year 2002 GISRA reporting included high-level management performance measures to assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific security requirements.

Limited security training for general users, IT professionals, and security professionals. OMB stated that through the administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were available to all federal agencies in late 2002.¹⁷ Initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers and the general workforce.

Inadequate integration of security into the capital planning and investment control process. OMB continues to address this issue through the budget process to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Further, OMB stated that through this process, agencies could demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. OMB also provided agencies with guidance in determining the security costs of their IT investments.

Poor security for contractor-provided services. Through the administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board (since eliminated), an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. This issue is currently under review by the Federal Acquisition Regulatory Council to develop, for governmentwide use, a clause to ensure that security is appropriately addressed in contracts.

Limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections. OMB stated that addressing this weakness begins through incident detection and reporting by individual agencies to incident response centers at the Department of Homeland Security (DHS), the FBI, the Department of Defense, or elsewhere. OMB also

¹⁷Launched in July 2002 by the Office of Personnel Management, the www.golearn.gov site offers training in an online environment.

noted that agencies must actively install corrective patches for known vulnerabilities and reported that the Federal Computer Incident Response Center (FedCIRC) awarded a contract on patch management to disseminate patches to all agencies more effectively.¹⁸ Among other actions, OMB and the CIO Council have developed and deployed a process to rapidly identify and respond to cyber threats and critical vulnerabilities.

Although not highlighted in OMB's report, in our April 2003 testimony before this subcommittee, we identified other activities undertaken to address these common weaknesses.¹⁹ In particular, during the past year, NIST has issued related security guidance, including

- draft guidelines on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program;²⁰
- a draft guide on security considerations in federal IT procurements, including specifications, clauses, and tasks for areas such as IT security training and awareness, personnel security, physical security, and security features in systems;²¹ and
- procedures for handling security patches that provided principles and methodologies for establishing an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.²²

In addition to these identified weaknesses, in its fiscal year 2001 report, OMB stated that it would direct all large agencies to undertake a Project Matrix review to more clearly identify and prioritize the security needs for government assets. Project Matrix is a methodology developed by the Critical Infrastructure

¹⁸FedCIRC, 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. FedCIRC introduced its Patch Authentication and Dissemination Capability Program in January 2003 as a free service to federal civilian agencies. According to FedCIRC, this service provides a trusted source of validated patches and notifications on new threats and vulnerabilities that have potential to disrupt federal government mission critical systems and networks. It is a Web-enabled service that obtains patches from vendors, validates that the patch only does what it states that it was created to correct, and provides agencies notifications based on established profiles.

¹⁹GAO-03-564T.

²⁰National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, NIST Draft Special Publication 800-50 (July 19, 2002).

²¹National Institute of Standards and Technology, *Security Considerations in Federal Information Technology Procurements: A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*, NIST Draft Special Publication 800-4A (Oct. 9, 2002).

²²National Institute of Standards and Technology, *Procedures for Handling Security Patches—Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (August 2002).

Assurance Office (CIAO) (recently transferred to the Department of Homeland Security) that identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.²³ OMB reported that once reviews have been completed at each large agency, it would identify cross-government activities and lines of business for Project Matrix reviews so that it will have identified both vertically and horizontally the critical operations and assets of the federal government's critical enterprise architecture and their relationship beyond government. In its fiscal year 2002 report, OMB acknowledged this requirement, but did not assess agencies' overall progress or indicate a goal for when this process will be complete. As we testified in April 2003, 14 agencies reported they had identified their critical assets and operations—10 using Project Matrix and 4 using other methodologies. Five more agencies reported that they were in some stage of identifying their critical assets and operations, and three more planned to do so in fiscal year 2003. However, this process may take several more years to complete because OMB has not established any deadlines for the completion of Project Matrix reviews.

OMB's fiscal year 2002 report also identifies several additional governmentwide issues and trends as concerns. These are as follows:

- Agencies identify the same security weaknesses year after year, such as a lack of system-level security plans. OMB reports that it will assist agencies in prioritizing and reallocating funds to address these problems.
- Some IGs and CIOs have vastly different views of the state of the agency's security programs, and OMB reports that it will highlight such discrepancies to agency heads.
- Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB reports that it will assist agencies in reprioritizing their resources through the budget process.
- Based on the information in the reports, not all agencies are successfully reviewing all programs and systems each year, as required by information security law.

²³The Project Matrix methodology defines "critical" as the responsibilities, assets, nodes, and networks that, if incapacitated or destroyed, would jeopardize the nation's survival; have a serious, deleterious effect on the nation at large; adversely affect large portions of the American populace; and require near-term, if not immediate, remediation (currently defined as within 72 hours). It defines "assets" as tangible equipment, applications, and facilities that are owned, operated, or relied upon by the agency, such as information technology systems or networks, buildings, vehicles (aircraft, ships, or land), satellites, or even a team of people.

-
- More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure, rather than thinking of IT security as the responsibility of a single agency official or the agency's IT security office.

As part of its fiscal year 2002 report, OMB listed five areas in which it will continue to work with agencies to ensure progress in safeguarding the federal government's information and systems: (1) the plan of action and milestones process, (2) IT security performance measures, (3) the President's Management Agenda Scorecard, (4) governmentwide milestones for IT security, and (5) the threat and vulnerability response process. Key actions identified for these areas include the following:

- To ensure that remediation plans continue to be developed, implemented, and corrective actions prioritized and tracked, OMB guidance will instruct IGs, as part of their fiscal year 2003 FISMA work, to assess whether each agency has in place a robust agencywide plan of action and milestone process. A robust process, verified by agency IGs, is one of three criteria agencies must meet to "get to green" for security on the Expanding E-Government Scorecard.
- To assist agencies and OMB in better tracking progress, along with their plan of action and milestone updates, agencies will also be required to begin quarterly reporting of their status against the OMB-prescribed IT security performance measures.
- OMB set targeted milestones for improvement for some of the critical IT security weaknesses in the President's FY 2004 budget. Targets for improvement include that by the end of 2003
 - all agencies are to have an adequate agencywide process in place for developing and implementing program- and system-level plans,
 - 80 percent of federal IT systems shall be certified and accredited, and
 - 80 percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the life cycle of the investment.

Agencies Show Limited Progress in Implementing Security Requirements

Our analyses of agency performance measure data and individual agencies' efforts to implement information security requirements showed limited progress in many cases. This limited progress is indicated despite other benefits that have resulted from GISRA implementation, such as increased management attention to and accountability for information security; important actions by the administration, such as integrating information security into the President's Management Agenda Scorecard; an increase in the types of information being reported and made available for oversight; and the establishment of a baseline for measuring agencies' performance.²⁴

As mentioned previously, for fiscal year 2002 OMB required agencies to report performance measure data related to key information security requirements, such as assessing systems for risk and having up-to-date system security plans. Summarizing these data for 24 large federal agencies and comparing results between fiscal years 2001 and 2002, OMB reported in its fiscal year 2002 report that these data indicated that agencies had made significant progress. Table 1 shows the governmentwide results of this analysis reported by OMB for selected performance measures, which indicates improvements for these measures ranging from 18 to 27 percentage points.

Table 1: Comparison of Fiscal Year 2001 and Fiscal Year 2002 Performance Measure Data for 24 Large Federal Agencies

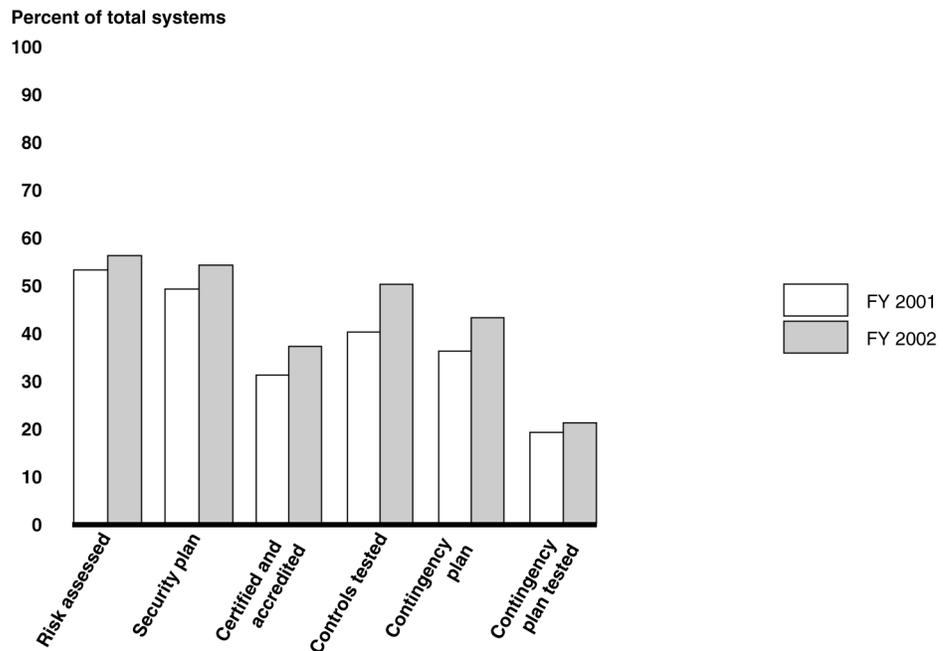
Year	Number of systems													
	Total		Assessed for risk and assigned a level of risk		Have an up-to-date IT security plan		Authorized for processing following certification & accreditation		Security controls have been tested and evaluated in the last year		Have a contingency plan		Contingency plan has been tested	
	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
Number of systems	7,411	7,957	3,195	5,160	2,986	4,930	1,953	3,772	2,447	4,751	2,221	4,342	1,228	2,768
Percentage of total systems			43	65	40	62	26	47	33	60	30	55	17	35
Difference from FY01 to FY02	+546 systems		+22%		+22%		+21%		+27%		+25%		+18%	

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

²⁴U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002); GAO-03-564T.

However, our analyses showed that most agencies experienced more limited progress than the OMB analysis indicates. Specifically, excluding data for the National Aeronautics and Space Administration (NASA), our analysis showed that increases for these same measures only ranged from 3 to 10 percent. NASA's performance measure data were excluded because fiscal year 2001 data were based on a sample of 221 of its most critical systems, but were compared with data for its total of 1,641 systems for fiscal year 2002. As a result, including NASA data significantly affected the overall levels of governmentwide progress shown. Figure 1 shows the percentage change in performance measures based on our analysis, excluding data for NASA.

Figure 1: Performance Measure Percentages for Selected Information Security Requirements^a



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform and GAO (analysis).
^aExcludes data for NASA.

In addition to the impact of the NASA data, the performance data reported by the Department of Defense (DOD) also represents only a small sample of the thousands of systems DOD identified in total for the department, and could significantly affect overall governmentwide results if data on all systems were available. DOD reported that because of its size and complexity, the collection of specific metrics required sizable lead time to allow for the collection and approval process by each military service and agency. For this reason, DOD focused its

fiscal year 2002 GISRA efforts on (1) a sample of 366 of its networks and (2) a sample of 155 systems that were selected from the sample of systems used for DOD's fiscal year 2001 GISRA review. It is these 155 systems for which DOD reported performance measure data.

In addition to the our analysis of these overall performance measures, we analyzed fiscal year 2002 GISRA reports by the 24 agencies and focused on the status of individual agencies in implementing federal information security requirements related to these and other measures. These analyses showed mixed agency progress but overall, many agencies still had not established information security programs that implement these requirements for most of their systems. Summaries of our analyses for selected information security requirements and reported performance measures follow.²⁵

Many Systems Do Not Have Risk Assessments

Agencies are required to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.²⁶ Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not developed on the basis of risk. As a result, the agencies had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.

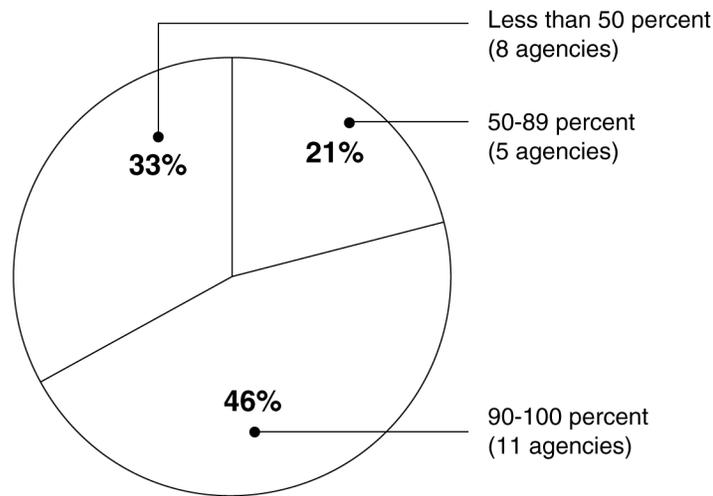
OMB's performance measure for this requirement mandated that agencies report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. Our analyses of reporting for this measure showed some overall progress. For example, of the 24 agencies, 13 reported an increase in the percentage of systems assessed for fiscal year 2002 compared with fiscal year 2001. In addition, as illustrated in figure 2, for fiscal

²⁵In performing our analyses, we summarized and categorized the reported information including data provided for the OMB-prescribed performance measures. There were several instances where agency reports either did not address or provide sufficient data for a question or measure. In addition, IGs' independent evaluations sometimes showed different results than CIO reporting or identified data inaccuracies. Further, IG reporting also did not always include comparable data, particularly for the performance measures. In part, this was because although OMB instructions said that the IGs should use the performance measures to assist in evaluating agency officials' performance, the IG was not required to review the agency's reported measures.

²⁶GAO/AIMD-98-68.

year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems. However, figure 2 also shows that further efforts are needed by other agencies, including the 8 that reported that less than 50 percent of their systems had been assessed for risk.

Figure 2: Percentage of Systems with Risk Assessments during Fiscal Year 2002



Source: Agency-reported data.

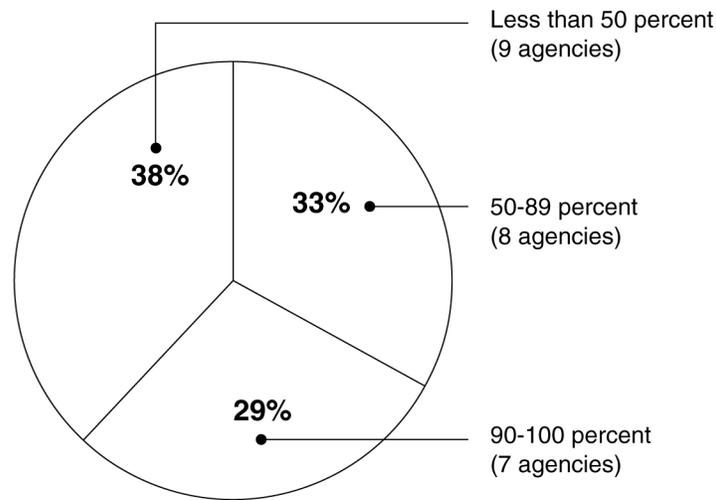
Systems Lack Up-to-Date Security Plans

An agency head is required to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle. Agencies also had to report the number and percentage of systems that had an up-to-date security plan. Our analyses showed that although most agencies reported that they had taken such actions, IG reports disagreed for a number of agencies, and many systems do not have up-to-date security plans. Specifically, 21 agencies reported that the agency head had taken actions to oversee that security plans are up to date and practiced throughout the life cycle. In comparison, of the 21 IGs that addressed this issue, 9 reported such actions had been taken and 12 reported that they had not. One IG reported that the agency's security plan guidance

predates revisions to NIST and OMB guidance and, as a result, does not contain key elements, such as the risk assessment methodology used to identify threats and vulnerabilities. In addition, another IG reported that although progress had been made, security plans had not been completed for 62 percent of the agency's systems.

Regarding the status of agencies' security plans, as shown in figure 3, 9 of the 24 agencies reported that they had up-to-date security plans for less than 50 percent of their systems for fiscal year 2002. Of the remaining 15 agencies, 7 reported up-to-date security plans for 90 percent or more of their systems.

Figure 3: Percentage of Systems with Up-to-Date Security Plans during Fiscal Year 2002



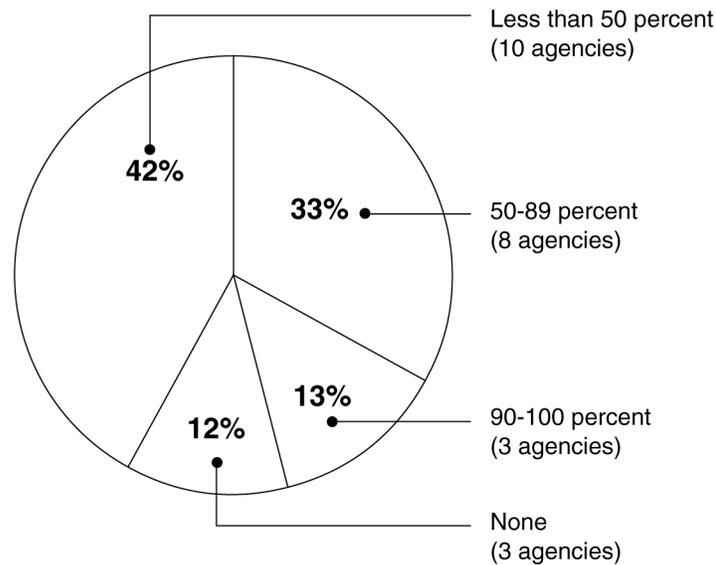
Source: Agency-reported data.

System Certification and Accreditation Remains a Problem

As one of its performance measures for agency program official responsibilities, OMB required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. Our analysis of agencies' reports showed mixed progress for this measure. For example, 10 agencies reported increases in the percentage of systems authorized for processing following certification and accreditation compared with fiscal year

2001, but 8 reported decreases and 3 did not change (3 others did not provide sufficient data). In addition, as shown in figure 4, 11 agencies reported that for fiscal year 2002, 50 percent or more of their systems had been authorized for processing following certification and accreditation, with only 3 of these reporting from 90 to 100 percent. And of the remaining 13 agencies reporting less than 50 percent, 3 reported that none of their systems had been authorized.

Figure 4: Percentage of Systems during Fiscal Year 2002 that are Authorized for Processing by Management after Certification and Accreditation



Source: Agency-reported data.
Note: Rounding used to total 100 percent.

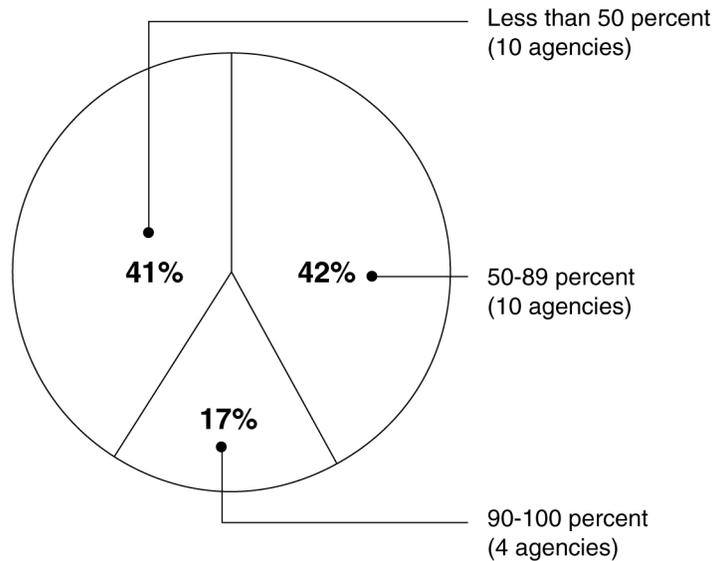
In addition to this mixed progress, IG reports identified instances in which agencies' certification and accreditation efforts were inadequate. For example, one agency reported that 43 percent of its systems were authorized for processing following certification and accreditation. IG reporting agreed, but also noted that over a quarter of the systems identified as authorized had been operating with an interim authorization and did not meet all of the security requirements to be granted accreditation. The IG also stated that, due to the risk posed by systems operating without certification and full accreditation, the department should consider identifying this deficiency as a material weakness.

Further Security Control Testing and Evaluation Needed

An agency head is responsible for ensuring that the appropriate agency officials evaluate the effectiveness of the information security program, including testing controls. Further, the agencywide information security program is to include periodic management testing and evaluation of the effectiveness of information security policies and procedures. 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 the program reviews can supplement 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 required agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. Our analyses of the data agencies reported for this measure showed that although 15 agencies reported an increase in the overall percentage of systems being tested and evaluated for fiscal year 2002, most agencies are not testing all of their systems. As shown in figure 5, our analyses showed that 10 agencies reported that they had tested the controls of less than 50 percent of their systems for fiscal year 2002. Of the remaining 14 agencies, 4 reported that they had tested and evaluated controls for 90 percent or more of their systems.

Figure 5: Percentage of Systems with Security Controls Tested during Fiscal Year 2002



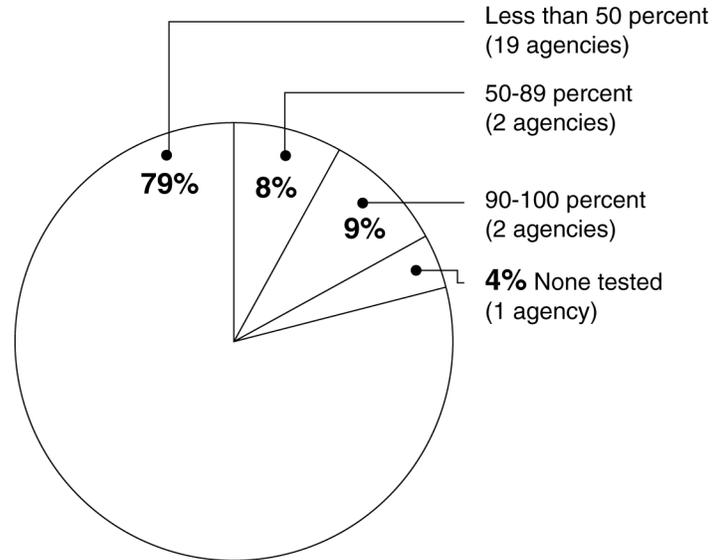
Source: Agency-reported data.
Note: Rounding used to total 100 percent.

Lack of Contingency Plan Testing Is a Major Weakness

Contingency plans provide specific instructions for restoring critical systems, including such items as arrangements for alternative processing facilities, in case the usual facilities are significantly damaged or cannot be accessed. At many of the agencies we have reviewed, plans and procedures to ensure that critical operations can continue when unexpected events occur, such as temporary power failure, accidental loss of files, or major disaster, were incomplete. These plans and procedures were incomplete because operations and supporting resources had not been fully analyzed to determine which were critical and would need to be restored first. Further, existing plans were not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans have been tested in the past year. As shown in figure 6, our analyses indicated that for fiscal year 2002, only 2 agencies reported that they had tested contingency plans for 90 percent or more of their systems, and 19 had tested contingency plans for less than 50 percent of their systems. One reported that none had been tested.

Figure 6: Percentage of Systems with Recently Tested Contingency Plans for Fiscal Year 2002



Source: Agency-reported data.
Note: Rounding used to total 100 percent.

Security Training Efforts Show Mixed Progress

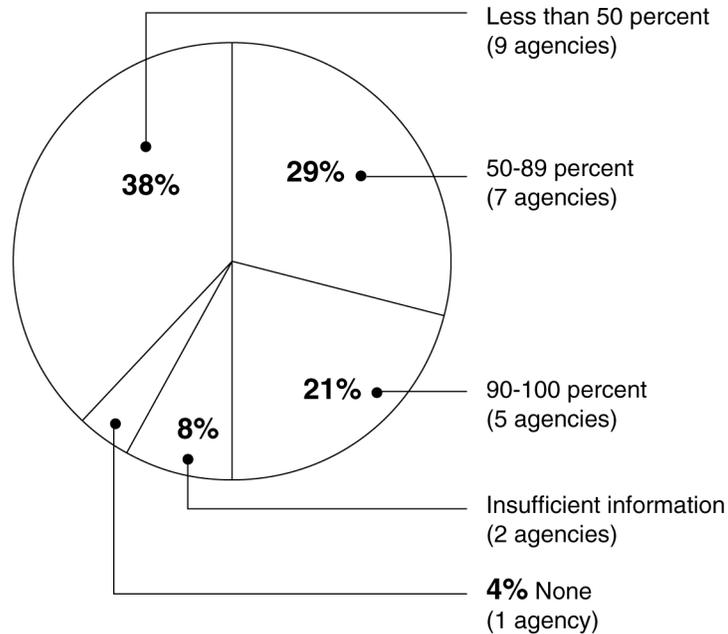
Agencies are required to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects 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. However, our past information security reviews at individual agencies have shown that they have not provided adequate computer security training to their employees, including contractor staff.

Among the performance measures for these requirements, OMB mandated that agencies report the number and percentage of employees—including contractors—who received security training during fiscal years 2001 and 2002, and the number of employees with significant security responsibilities who received specialized training. Our analyses showed that 16 agencies reported that they provided security training to 50 percent or more of their employees and

contractors for fiscal year 2002, with 9 reporting 90 percent or more. Of the remaining 8 agencies, 4 reported that such training was provided for less than half of their employees/contractors, 1 reported that none were provided with this training, and 3 provided insufficient data for this measure.

For specialized training for employees with significant security responsibilities, some progress was indicated, but additional training is needed. As indicated in figure 7, our analyses showed that 12 agencies reported that 50 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 reporting 90 percent or more. Of the remaining 12 agencies, 9 reported that less than half of such employees received specialized training, 1 reported that none had received such training, and 2 provided insufficient data for this measure.

Figure 7: Percentage of Employees with Significant Security Responsibilities Receiving Specialized Security Training during Fiscal Year 2002



Source: Agency-reported data.

Incident-Handling Capabilities Established, but Implementation Incomplete

Agencies are required to implement procedures for detecting, reporting, and responding to security incidents. 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 intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are 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. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management.

Our information security reviews also confirm that federal agencies have not adequately (1) prevented intrusions before they occur, (2) detected intrusions as they occur, (3) responded to successful intrusions, or (4) reported intrusions to staff and management. Such weaknesses provide little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage.

OMB included a number of performance measures in agency reporting instructions that were related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with FedCIRC in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner.

Our analyses of agencies' reports showed that although most agencies reported that they have established incident-response capabilities, implementation of these capabilities is still not complete. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities and 8 others reported that they provided these capabilities to components through a central point within the agency. However, although most agencies report having these capabilities for most components, in at least two cases, the IGs' evaluations identified instances in which incident-response capabilities were not always implemented. For example, one IG reported that the agency established and implemented its computer security incident-response capability on August 1, 2002, but had not enforced procedures to ensure that components comply with a consistent methodology to identify, document, and report computer security incidents. Another IG reported that the agency had

released incident-handling procedures and established a computer incident-response team, but had not formally assigned members to the team or effectively communicated procedures to employees.

Our analyses also showed that for fiscal year 2002, 13 agencies reported that they had oversight procedures to verify that patches had been tested and installed in a timely manner, and 10 reported that they did not. Of those that did not have procedures, several specifically mentioned that they planned to participate in FedCIRC's patch management process.

Some Reported Improvement in Efforts to Ensure Security of Contractor-Provided Services

Agencies are required to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained either by the agency or for it by another agency or contractor. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements.

Our analyses showed that a number of agencies reported that they have reviewed a large percentage of services provided by a contractor, but others have reviewed only a small number. For operations and assets under the control of agency program officials, 17 agencies reported that for fiscal year 2002 they reviewed 50 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more. Four agencies reported that they had reviewed less than 30 percent of contractor operations or facilities.

For operations and assets under the control of the CIO, 13 agencies reported that for fiscal year 2002 they reviewed 50 percent or more of contractor operations or facilities, with 7 of these reporting that they reviewed 90 percent or more. Of the remaining agencies, 3 reported that they reviewed less than 30 percent of contractor operations or facilities and 5 reported that they had no services provided by a contractor or another agency.

Processes Needed to Ensure Effective Corrective Actions

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. OMB has required agency heads to work with CIOs and program officials to provide a strategy to correct security weaknesses identified through annual program reviews and independent evaluations, as well as other reviews or audits performed throughout the reporting period by the IG or us. Agencies are also required to submit corrective action plans for all programs and systems where a security weakness has been identified. OMB guidance requires that these plans list the identified weaknesses and, for each, identify a point of contact, the resources required to resolve the weakness, the scheduled completion date, key milestones with completion dates for the milestones, milestone changes, the source of the weakness (such as a program review, IG audit, or GAO audit), and the status (ongoing or completed). Agencies are also required to submit quarterly updates of these plans that list the total number of weaknesses identified at the program and system levels, as well as the numbers of weaknesses for which corrective actions were completed on time, ongoing and on schedule, or delayed. Updates are also to include the number of new weaknesses discovered subsequent to the last corrective action plan or quarterly update.

As reported in its fiscal year 2002 report to the Congress, OMB requires that agencies establish and maintain an agencywide process for developing and implementing program- and system-level corrective action plans and that these plans serve as an agency's authoritative management tool to ensure that program- and system-level IT security weaknesses are remediated. In addition, OMB requires that every agency maintain a central process through the CIO's office to monitor agency remediation activity.

Our analyses of agencies' fiscal year 2002 corrective action plans, IGs' evaluations of these plans, and available quarterly updates showed that the usefulness of these plans as part of agency management's overall process to identify and correct their information security weaknesses could be limited when they do not identify all weaknesses or provide realistic completion estimates. For example, of 14 agency IGs that reported on whether or not their agency's corrective action plan addressed all identified significant weaknesses, only 5 reported that their agency's plan did so, and 9 specifically reported that their agency's plan did not. Further, in several instances, corrective action plans did not indicate the current status of weaknesses identified or include information regarding whether actions were on track as originally scheduled.

In addition, most agencies did not indicate the relative priority of weaknesses for corrective action. As a result, it was difficult to determine whether an agency's actions are focused on achieving results for its most significant weaknesses. Further, three IGs reported that their agencies did not have a centralized tracking system to monitor the status of corrective actions, and one IG specifically questioned the accuracy of unverified, self-reported corrective actions reported in the agency's plan.

In its report, OMB highlighted several actions that may help to address such concerns. For example, OMB reported that since completion of their fiscal year 2002 reviews, agencies have been working to prioritize their IT security weaknesses. In addition, OMB stated that fiscal year 2003 FISMA reporting guidance would direct agency IGs to verify whether an agency has a central process to monitor remediation, as required by OMB.

Agencies Face Continuing Challenges to Implement Effective Information Security Management Programs

The governmentwide weaknesses identified by OMB in its reports to the Congress, as well as the limited progress in implementing key information security requirements, continue to emphasize that agencies have not effectively implemented programs for managing information security. For the past several years, we have analyzed the audit results for 24 of the largest federal agencies and found that all 24 had significant weaknesses in the policies, procedures, and technical controls that apply to all or a large segment of their information systems and help ensure their proper operation. In particular, our analyses in both 2001 and 2002 found that all 24 had weaknesses in security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls. Security program management covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.²⁷

Establishing a strong security management program requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and

²⁷U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001); and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002).

sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations*.²⁸ Our study found that these organizations managed their information security risks through a cycle of risk management activities. These activities, which are now among the federal government's statutory information security requirements, included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet those needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

Although GISRA reporting provides performance information on these areas, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security. Also, development of management strategies that identify specific actions, time frames, and required resources may help to significantly improve performance.

FISMA Provisions Can Strengthen Information Security Implementation

With GISRA expiring on November 29, 2002, FISMA was enacted on December 17, 2002, to permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA. In particular,

²⁸GAO/AIMD-98-68.

FISMA provisions established additional requirements that can assist the agencies in implementing effective information security programs, help ensure that agency systems incorporate appropriate controls, and provide information for administration and congressional oversight. These specific requirements are described and discussed below.

Designating a Senior Agency Information Security Officer

FISMA 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.

In contrast, GISRA required the CIO to designate a senior agency information security official, but did not specify the responsibilities, qualifications, or other requirements for this position. Agencies' fiscal year 2002 GISRA reports showed that the CIOs had designated a senior agency information security official for 22 of the 24 agencies (the remaining 2 agencies' reports did not indicate whether they had designated such an official), but OMB did not require the agencies to report any additional information on the responsibilities of this official.

Developing, Maintaining, and Updating an Inventory of Major Information Systems

FISMA requires each agency to 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 also 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. FISMA also mandates that OMB issue guidance and oversee the

implementation of this requirement. Although GISRA did not specifically require that agencies maintain an inventory of major information systems, OMB reporting instructions for fiscal year 2002 did require agencies to report the total number of agency systems, and most agencies reported a total number in their GISRA reports. However, six IGs specifically reported problems with the completeness of their agencies' system inventories.

NIST Development of Standards and Guidelines

FISMA includes a number of requirements for NIST to develop security-related standards and guidelines. These include, for systems other than those dealing with national security, (1) standards to be used by all agencies to categorize all of 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.

For the first of these requirements—standards for security categorization—NIST is to submit the standards to the Secretary of Commerce for promulgation no later than 12 months after enactment (December 17, 2003). The guidelines on the types of information and information systems to be included in each category are required to be issued no later than 18 months after enactment (June 17, 2004). The minimum information security requirements are required to be submitted to the Secretary for promulgation no later than 36 months after enactment (December 17, 2005).

On May 16, 2003, NIST issued an initial public draft of the standards for security categorization for comment.²⁹ These proposed standards would establish three levels of risk—**low**, **moderate**, and **high**³⁰—and would categorize information and

²⁹National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199, Initial Public Draft, Version 1.0, May 2003.

³⁰As defined in the draft NIST standard, the level of risk is **low** if an event could be expected to have a limited adverse effect on agency operations (including mission, functions, image or reputation), agency assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs. The level of risk is **moderate** if an event could be expected to have a serious adverse effect on agency operations, agency assets, or individuals; and cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs. The level of risk is **high** if an event could be expected to have a severe or catastrophic adverse effect on agency operation, agency assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

information systems with respect to security by having an agency assign the appropriate level of risk to each of three security objectives: (1) **confidentiality**, defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; (2) **integrity**, defined as guarding against improper information modification or destruction, and including ensuring information nonrepudiation and authenticity; and (3) **availability**, defined as ensuring timely and reliable access to and use of information. Also according to the draft standard, because an information system may contain more than one type of information that is subject to security categorization (such as privacy information, medical information, proprietary information, financial information, and contractor-sensitive information), the security categorization of an information system that processes, stores, or transmits multiple types of information should be at least the highest risk level that has been determined for each type of information for each security objective, taking into account dependencies among the objectives.

FISMA also requires NIST to develop, in conjunction with the Department of Defense, including the National Security Agency, guidelines for identifying an information system as a national security system. On June 3, 2003, NIST released a draft working paper of these guidelines that provides the basis and method for identifying national security systems, including agency determination and reporting responsibilities.³¹

Agency Reporting to the Congress

For non-national-security programs, GISRA required those performing the annual independent evaluations (essentially the IGs) to report the results of their evaluations to OMB and required OMB to summarize these results in an annual report to the Congress. In addition, OMB required the agencies to report the results of their annual GISRA security reviews of systems and programs. FISMA now requires agencies to report annually to OMB, as well as to the House Committees on Government Reform and Science; the Senate Committees on Governmental Affairs and Commerce, Science, and Transportation; the appropriate congressional authorizing and appropriations committees; and the Comptroller General; on the adequacy and effectiveness of information security policies, procedures, and practices, including compliance with each of FISMA's requirements for an agencywide information security program.

³¹National Institute of Standards and Technology, *Guideline for Identifying an Information System as a National Security System*, NIST Special Publication 800-59, Draft, Version 0.3, June 3, 2003.

In summary, with few exceptions, agencies' implementation of federal information security requirements has not yet shown significant progress. Legislation, congressional oversight like today's hearing, and efforts by OMB through the budget process, the President's Management Agenda Scorecard, and other tools, such as corrective action plans and performance measures, have all contributed to increasing agency management's attention to information security. Also, new techniques, such as establishing governmentwide performance goals and quarterly reporting of performance measures, may help to further encourage agency progress and facilitate congressional and administration oversight.

However, in addition to these steps, achieving significant and sustainable results will likely require agencies to integrate such techniques into overall security management programs and processes that prioritize and routinely monitor and manage their information security efforts. These programs and processes must focus on implementing statutory security requirements, including performing risk assessments, testing and evaluating controls, and identifying and correcting weaknesses to ensure that the greatest risks have been identified, security controls have been implemented to address these risks, and that critical operations can continue when unexpected events occur. Development of management strategies that identify specific actions, time frames, and required resources may also help to significantly improve performance. 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 pleased to answer any questions that you or other 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. I can also be reached by E-mail at dacey@gao.gov.

(310194)