United States Government Accountability Office

GAO

Testimony

Before the House Committee on Government Reform

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, March 16, 2006

INFORMATION SECURITY

Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues

March 16, 2006

INFORMATION SECURITY

Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-527T, a testimony to the House Committee on Government Reform

Why GAO Did This Study

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

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

This testimony discusses:

- The federal government's progress and challenges in implementing FISMA, as reported by the Office of Management and Budget (OMB), the agencies, and the Inspectors General (IGs).
- Actions needed to improve FISMA reporting and address underlying information security weaknesses.

www.gao.gov/cgi-bin/getrpt?GAO-06-527T.

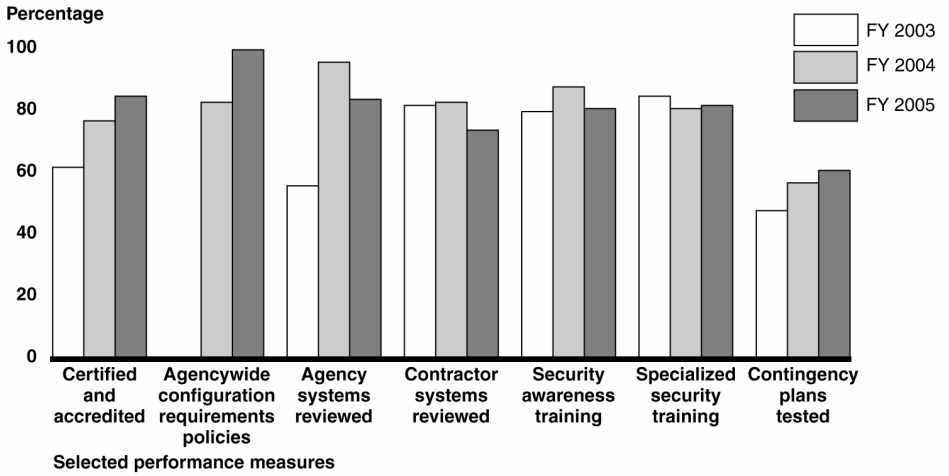
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In its fiscal year 2005 report to Congress, OMB discusses progress in implementing key information security requirements, but at the same time cites challenging weaknesses that remain. The report notes several governmentwide findings, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation (the process of authorizing operation of a system, including the development and implementation of risk assessments and security controls). Nevertheless, fiscal year 2005 data reported by 24 major agencies, compared with data reported for the previous 2 fiscal years (see fig.), show that these agencies have made steady progress in certifying and accrediting systems, although they reported mixed progress in meeting other key statutory information security requirements. For example, agencies reported that only 61 percent of their systems had tested contingency plans, thereby reducing assurance that agencies will be able to recover from the disruption of those systems with untested plans.

Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses. OMB has taken several actions to improve FISMA reporting—such as requiring agencies to provide performance information based on the relative importance or risk of the systems—and can further enhance the reliability and quality of reported information. Agencies also can take actions to fully implement their FISMA-mandated programs and address the weaknesses in their information security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are to prevent, limit, and detect access to the agencies' information and information systems.

Reported Data for Selected Performance Measures for 24 Major Agencies



Source: GAO analysis of agencies' FY2003-2005 FISMA reports.

Mr. Chairman and Members of the Committee:

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

In my testimony today, I will summarize our analysis of the reported status of the federal government's implementation of FISMA. I will note areas where the agencies have made progress in implementing the requirements of the Act and those areas where weaknesses remain. I will also touch on additional actions that federal entities can take to help fully implement the mandated information security programs and to improve the effectiveness of information security controls.

In conducting this work, we reviewed and summarized OMB's fiscal year 2005 report to Congress on FISMA implementation, dated March 1, 2006. We also analyzed and summarized the fiscal year

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

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

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

2005 FISMA reports from 24 major federal agencies[4] and their inspectors general (IGs). In addition, we reviewed standards and guidance issued by OMB and the National Institute of Standards and Technology (NIST) pursuant to their responsibilities under the Act. We did not validate the accuracy of the data reported by the agencies or OMB, but we did analyze the IGs' fiscal year 2005 FISMA reports to identify any issues related to the accuracy of agency-reported information. Finally, we examined and summarized key findings of related GAO products. We performed our work from October 2005 to March 2006 in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2005 report to Congress, OMB noted that the federal government has made progress in meeting key performance measures for information security; however, uneven implementation of security efforts has left weaknesses in several areas. OMB identified weaknesses with the extent of agencies' oversight of contractor systems, testing of security controls, and reporting of security incidents, as well as the quality of agencies' plans of action and milestones and certification and accreditation processes. The report presented a plan of action that OMB is pursuing with federal agencies to improve their management of information security.

The fiscal year 2005 reports submitted by the agencies present a mixed picture of FISMA implementation in the federal government. In their fiscal year 2005 reports, 24 major federal agencies generally reported an increasing number of systems meeting key information security performance measures, such as percentage of systems certified and accredited and percentage of contingency plans tested.

[4] These 24 departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, 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.

Nevertheless, progress was uneven. For example, the percentage of agency systems reviewed declined from 96 percent in 2004 to 84 percent in 2005, and the percentage of employees and contractors receiving security awareness training also declined, from 88 percent in 2004 to 81 percent in 2005.

Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses. OMB has taken several actions to improve FISMA reporting — such as requiring agencies to indicate the relative importance or risk level of their systems — and can further enhance the reliability and quality of reported information. Agencies can also take actions to fully implement their FISMA-mandated programs and address the weaknesses in their information security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are designed to prevent, limit, and detect access to the agencies' information and information systems.

Background

Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While this interconnectivity offers us huge benefits, without proper safeguards it also poses significant risks to the government's computer systems and, more importantly, to the critical operations and infrastructures they support. We reported in 2005 that while federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses in federal computer systems that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction,

sensitive information at risk of inappropriate disclosure, and critical operations at the risk of disruption.[5]

The significance of these weaknesses led us to conclude in the audit of the federal government's fiscal year 2005 financial statements[6] that information security was a material weakness.[7] Our audits also identified instances of similar types of weaknesses in non-financial systems.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is high. The weaknesses we 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 other computer systems.
- Sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of industrial espionage or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.

[5]GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[6]GAO, *Fiscal Year 2005 U.S. Government Financial Statements: Sustained Improvement and Financial Management is Crucial to Addressing our Nation's Financial Conditions and Long-term Fiscal Imbalance*, GAO-06-406T (Washington, D.C.: March 1, 2006).

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

- Data could be modified or destroyed for purposes of fraud, identity theft, or disruption.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in federal organizations' abilities 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 and assets.

FISMA Authorized and Strengthened Information Security Requirements

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

Overall, FISMA requires each agency (including agencies with national security systems) to develop, document, and implement an agencywide information security program. This program should provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system, including minimally acceptable system configuration requirements;

- 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 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) that are 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.

Each agency is also required to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency IG or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head. The agencies are to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies,

procedures, practices, and compliance with FISMA requirements. In addition, agency heads are required to make annual reports of the results of their independent evaluations to OMB. OMB must submit a report to Congress no later than March 1 of each year on agency compliance, including a summary of the findings of agencies' independent evaluations.

Other major provisions direct that the National Institute of Standards and Technology (NIST) 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.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

OMB provides instructions to the agencies and their IGs on the annual FISMA reporting requirements. OMB's fiscal year 2005 reporting instructions, similar to the 2004 instructions, have a strong focus on performance measures. OMB has developed performance measures in the following areas:

- certification and accreditation,[8]
- testing of security controls,
- agency systems and contractor systems reviewed annually,
- testing of contingency plans,
- incident reporting,

[8]Agency management officials are required to 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.

- annual security awareness training for employees and contractors,
- annual specialized training for employees with significant security responsibilities, and
- minimally acceptable configuration requirements.

Further, OMB has provided instructions for continued agency reporting on the status of remediation efforts through plans of action and milestones. Required for all programs and systems where an IT security weakness has been found, these plans list the weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions. The plans are to be submitted twice a year to OMB. In addition, agencies are to submit quarterly updates that indicate the number of weaknesses for which corrective action has been completed as originally scheduled, or has been delayed, as well as the number of new weaknesses discovered since the last update.

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

OMB's Report to Congress Noted Improvements and Weaknesses

In its March 2006 report to Congress on fiscal year 2005 FISMA implementation,[9] OMB emphasized that the federal government has made progress in meeting key performance measures for IT security; however, uneven implementation of security efforts leaves weaknesses in several areas. OMB determined through its assessment of FISMA reports that advances have occurred at a governmentwide level in the following areas of IT security:

- *Systems certification and accreditation.* Agencies recorded a 19 percent increase in the total number of IT systems and reported that the percentage of certified and accredited systems rose from 77 percent in fiscal year 2004 to 85 percent in 2005. Moreover, OMB noted that 88 percent of systems assessed as high-risk have been certified and accredited.
- *Assessed quality of the certification and accreditation process*. OMB's analysis of reports from the IGs revealed an increase in agencies with a certification process rated as "satisfactory" or higher, from 15 in 2004 to 17 in 2005.
- *Plans of action and milestone process*. OMB noted that out of 25 agencies that it reviewed in detail,[10] 19 IGs report that their agencies have effective remediation processes, compared to 18 in 2004.

In addition to these areas of improvement, OMB detected areas with continuing weaknesses:

- *Contractor systems oversight.* IGs for 6 of 24 agencies (one agency IG did not respond) rated agency oversight of contractor systems in the "rarely" range, while 3 others rated this oversight in the next lowest range, "sometimes."

[9]Office of Management and Budget, *FY2005 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (Washington, D.C.: March, 2006).

[10]OMB includes the Smithsonian Institution in its list of major agencies. Our analysis in this testimony does not include the Smithsonian Institution.

- *Security controls testing*. Agencies tested the security controls on a lower percentage of systems, dropping from 76 percent in fiscal year 2004 to 72 percent in 2005. OMB noted a better rate of testing for high-risk systems, with a governmentwide total of 83 percent.
- *Incident reporting.* OMB stated that some agencies continue to report security incidents to the Department of Homeland Security only sporadically and that others report notably low levels of incidents.
- *Agencywide plans of action and milestones.* While IGs for 19 agencies reported effective POA&M processes, 6 others reported ineffective processes.
- *Certification and accreditation process.* OMB commented that while no IG rated the certification and accreditation process for its agency as failing, eight rated the process as "poor."

The OMB report also discusses a plan of action to improve performance, assist agencies in their information security activities, and promote compliance with statutory and policy requirements. OMB has set a goal for agencies to have 90 percent of their systems certified and accredited and their certification and accreditation process rated as "satisfactory" or better by their IGs.

Agency 2005 FISMA Reports Show Mixed Results

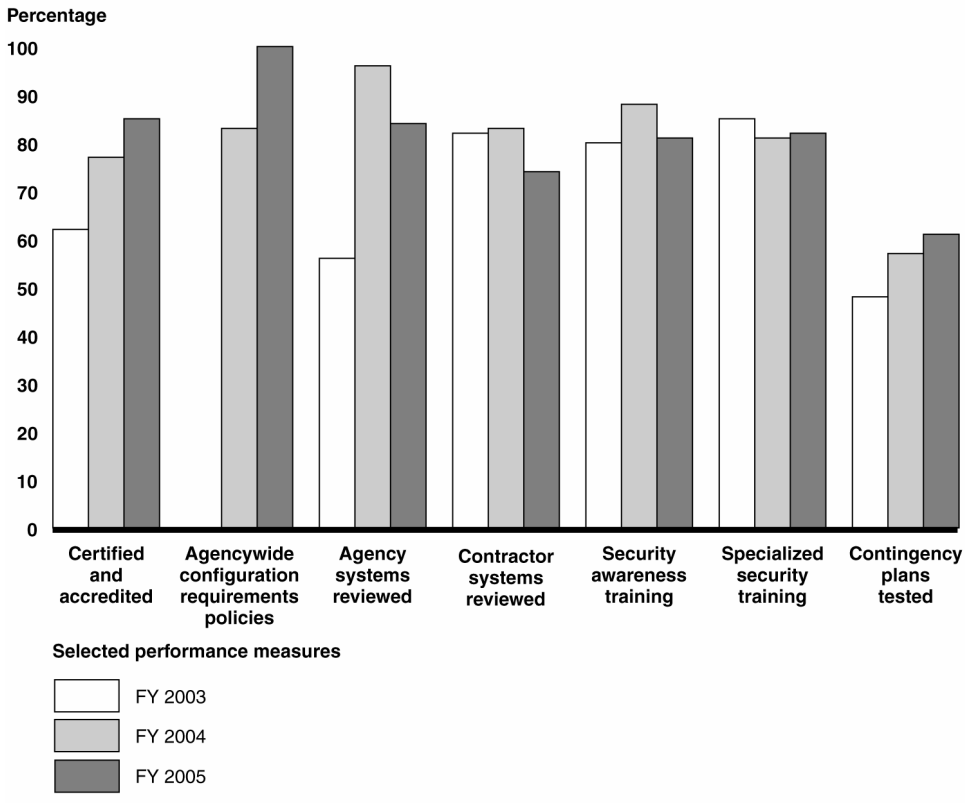
In their FISMA-mandated reports for fiscal year 2005, the 24 major agencies reported both improvements and weaknesses in major performance indicators. The following key measures showed increased performance and/or continuing challenges:

- percentage of systems certified and accredited;
- percentage of agencies with an agencywide minimally acceptable configuration requirements policy;
- percentage of agency systems reviewed annually;
- percentage of contractor systems reviewed annually;
- percentage of employees and contractors receiving annual security awareness training;
- percentage of employees with significant security responsibilities receiving specialized security training annually; and

- percentage of contingency plans tested.

Figure 1 illustrates that the major agencies have made steady progress in fiscal year 2005 certifying and accrediting their systems, although they have made mixed progress in meeting other key performance measures compared with the previous two fiscal years. Summaries of the results for specific measures follow.

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



Source: GAO analysis of agencies' FY2003-2005 FISMA reports.

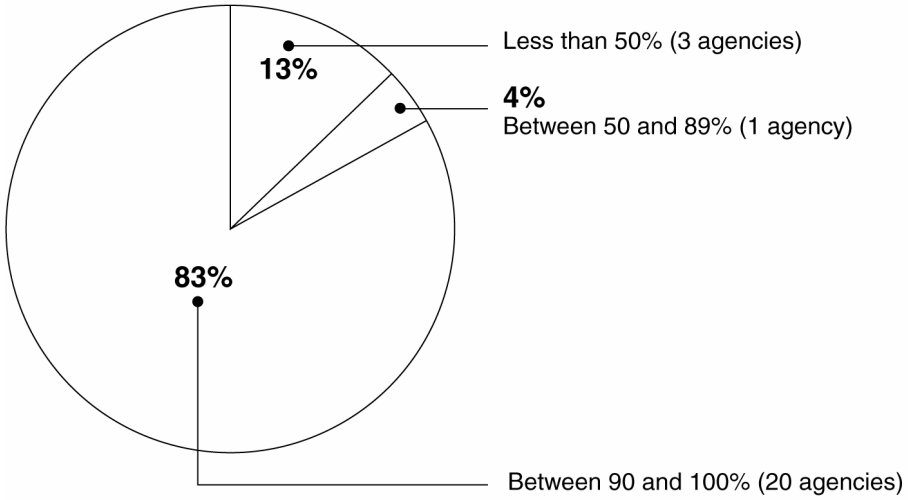
Certification and Accreditation

Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby

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

Data reported for this measure showed continued overall increases for most agencies over the last three years. For example, 15 agencies reported an increase in the percentage of their systems that had completed certification and accreditation. Overall, 85 percent of agencies' systems governmentwide were reported as certified and accredited in 2005, compared to 77 percent in 2004 and 62 percent in 2003. In addition, 20 agencies reported that 90 percent or more of their systems had successfully completed the process, as illustrated in figure 2.

Figure 2: Percentage of Agencies Reporting the Percentage of Their Systems that are Certified and Accredited for Processing in Fiscal Year 2005



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

Agencies appeared to appropriately focus their certification and accreditation efforts on high-risk systems. Agencies certified and

accredited a higher percentage of their high-risk systems (88 percent) than their moderate-risk systems.

Configuration Management

FISMA requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In fiscal year 2004, for the first time, agencies reported on the degree to which they had security configurations for specific operating systems and software applications. Our analysis of the 2005 agency FISMA reports found that all 24 major agencies reported that they had agencywide policies containing system configurations, an increase from the 20 agencies who reported having them in 2004. However, implementation of these requirements at the system level continues to be uneven. Specifically, 14 agencies reported having system configuration policies, but they did not always implement them on their systems.

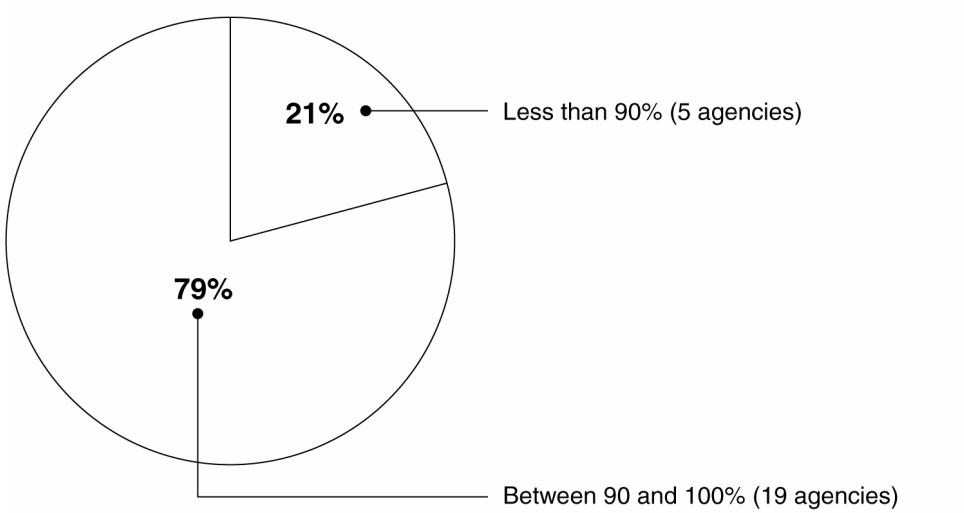
Annual Review of Agency Systems

FISMA requires that agency information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency that depends on risk, but no less than annually. This effort 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. In order to measure the performance of security programs, OMB requires that agencies report the number and percentage of systems that they have reviewed during the year.

Agencies reported a decrease in the percentage of their systems that underwent an annual review in 2005, after reporting major gains in this performance measure in 2004. In the 2005 reports, agencies stated that 84 percent of their systems had been reviewed in the last

year, as compared to 96 percent in 2004. While 23 agencies reported that they had reviewed 90 percent or more of their systems in 2004, 19 agencies reported this achievement in 2005, as shown in figure 3.

Figure 3: Percentage of Agencies Reporting the Percentage of Their Systems that have been Reviewed in Fiscal Year 2005



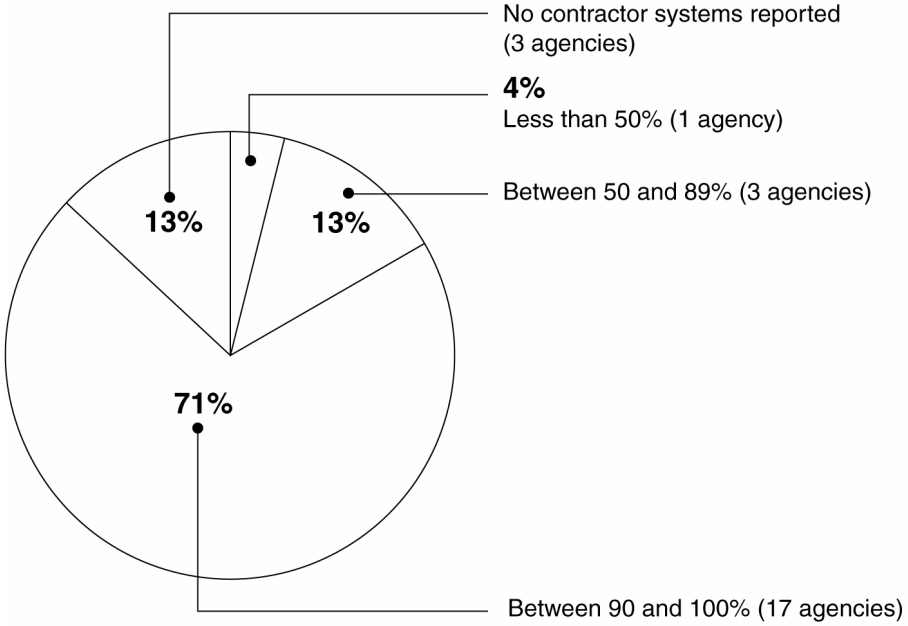
Source: Agency-reported data and GAO (analysis).

Annual Review of Contractor Systems

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. As OMB emphasized in its fiscal year 2005 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. According to longstanding OMB policy concerning sharing government information and interconnecting systems, federal security requirements continue to apply, and the agency is responsible for ensuring appropriate security controls.

The key performance measure of annual review of contractor systems by agencies decreased from 83 percent in 2004 to 74 percent in 2005, reducing the rate of reviews performed to below 2003 levels. However, the number of agencies that reported reviewing over 90 percent of their contractor systems has increased from 10 in 2004 to 17 in 2005. A breakdown of the percentages for fiscal year 2005 is provided in figure 4.

Figure 4: Percentage of Agencies Reporting the Percentage of Their Contractor Systems that have been Reviewed in Fiscal Year 2005



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

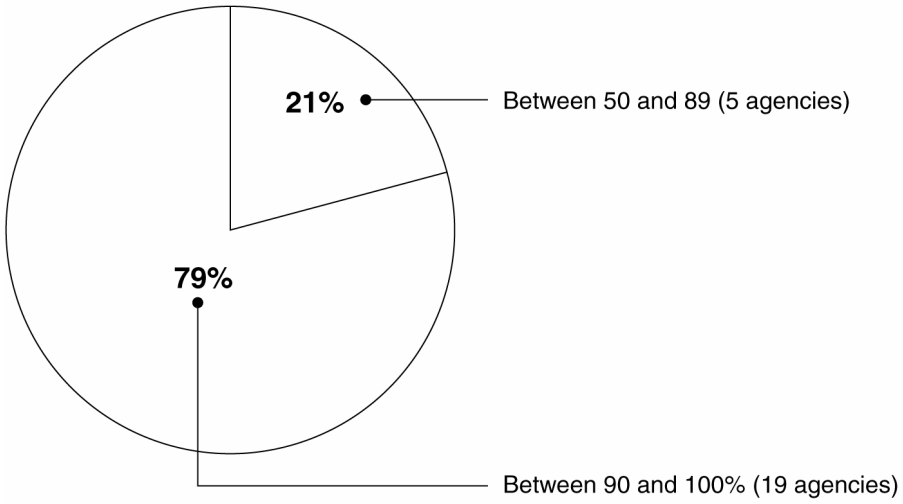
Although agencies reported that 74 percent of their contractor systems were reviewed in 2005, they only reviewed 51 percent of the contractor systems assessed as high-risk, as opposed to 89 percent of moderate-risk systems and 84 percent of low-risk systems. Without adequate contractor review, agencies cannot be assured that federal information held and processed by contractors is secure.

Security Awareness Training

FISMA requires agencies to provide security awareness training. This training should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and of the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading organizations[11] have shown that such organizations took steps to ensure that personnel involved in various aspects of information security programs had the skills and knowledge they needed.

In their FISMA submissions for fiscal year 2005, agencies reported that they provided security awareness training to the majority of their employees and contractors. However, while 19 agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness (see fig. 5), the overall percentage of employees trained among the 24 major federal agencies reviewed dropped from 88 percent in 2004 to 81 percent in 2005, a level almost equal to that reported in 2003.

Figure 5: Percentage of Agencies Reporting the Level of Their Employees and Contractors that have Received IT Security Awareness Training in Fiscal Year 2005



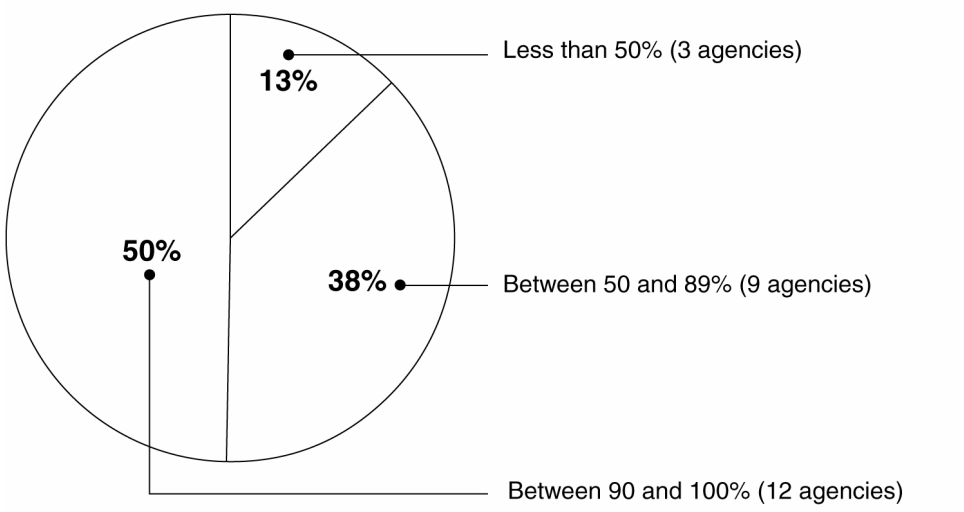
Source: Agency-reported data and GAO (analysis).

Specialized Security Training

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

Agencies reported varying levels of compliance in providing specialized training to employees with significant security responsibilities. Of the 24 agencies that we reviewed, 12 reported that they had provided specialized security training for 90 percent or more of these employees. (see fig. 6).

Figure 6: Percentage of Agencies Reporting the Level of Their Employees with Significant Security Responsibilities that have Received Specialized Security Training in Fiscal Year 2005



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

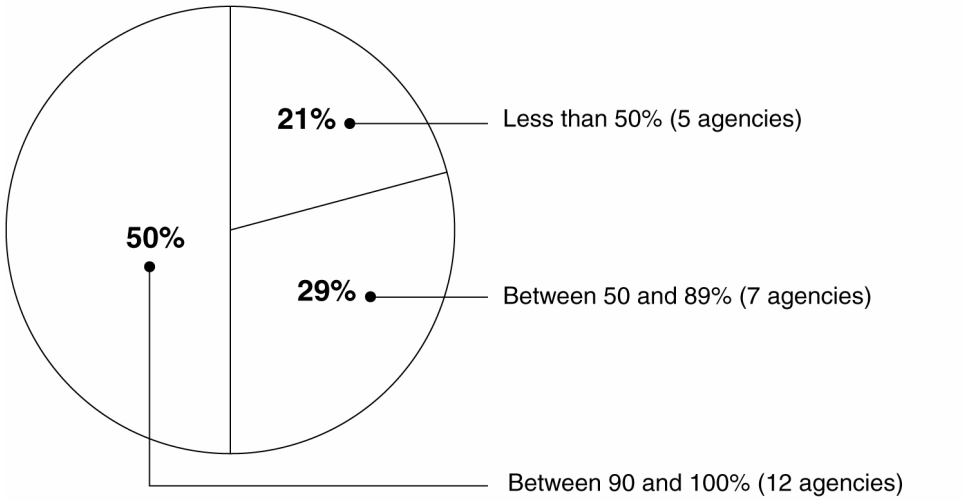
Although there was a gain of one point in the percentage of employees who received specialized security training for fiscal year 2005 (82 percent) over 2004 (81 percent), both of these years show a decrease from the level reported in 2003 (85 percent). Given the rapidly changing threats in information security, agencies need to keep their IT security employees up to date on changes in technology. Otherwise, agencies may face increased risk of security breaches.

Testing of Contingency Plans

Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed due to unexpected events such as a temporary power failure, the accidental loss of files, or a major disaster. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. The testing of contingency plans is essential to determining whether the plans will function as intended in an emergency, 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 to test overall service continuity. Such a test includes testing whether the alternative data processing site will function as intended and whether critical computer data and programs to be recovered from off-site storage will be accessible and current. In executing the plan, managers are able to identify weaknesses and make changes accordingly. Moreover, such tests assess how well employees have been trained to carry out their roles and responsibilities during a disaster. To show the status of implementing this requirement, OMB specifies that agencies report the number of systems with tested contingency plans.

Overall, agencies continued to report that they have not tested a significant number of their contingency plans with only 61 percent of systems with tested plans. Although this number continues to show small increases each year since 2003, figure 7 illustrates that 5 agencies reported less than 50 percent of their systems had tested contingency plans.

Figure 7: Percentage of Agencies Reporting the Level of Their Systems that have Tested Contingency Plans in Fiscal Year 2005



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

In addition, agencies do not appear to be appropriately prioritizing testing of contingency plans by system risk level, with high-risk systems having the lowest rate of systems with tested plans of the three risk levels. Without testing, agencies can have limited assurance that they will be able to recover mission critical applications, business processes, and information in the event of an unexpected interruption.

Inventory of Major Systems

FISMA requires that agencies develop, maintain, and annually update an inventory of major information systems operated by the agency, or under its control. 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. For the 2005 reports, OMB required agencies to report the number of major systems and asked the IGs about the status and accuracy of their agencies' inventories.

In 2005, agencies reported 10,261 systems, composed of 9,175 agency systems and 1,094 contractor systems. However, only 13 IGs reported that their agencies' inventories were substantially complete. A complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. Without reliable information on agencies' inventories, the agencies, the administration, and Congress cannot be fully assured of agencies' progress in implementing FISMA.

Risk Assessments

FISMA mandates that agencies assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure disruption, modification, or destruction of their information and information systems. The Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operation, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and is used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability. Once determined, security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. OMB's fiscal year 2005 reporting instructions included the new requirement that agencies report their systems and certain performance measures using FIPS 199 risk levels. If agencies did not categorize systems, or used a method other than FIPS 199 to determine risk level, they were required to explain why in their FISMA reports.

For the first time, in the 2005 reporting, agencies reported the risk levels for their agency and contractor systems, as illustrated in table 1.

Table 1: Systems Reported by Risk Level in Fiscal year 2005

Risk Level	Agency Systems	Percentage	Contractor Systems	Percentage	Overall Percentage
High-risk	1,646	18	293	27	19
Moderate-risk	2,493	27	249	23	27
Low-risk	4,446	49	164	15	45
Not categorized	580	6	390	35	9
Totals	9,165	100	1,096	100	100

Source: GAO analysis.

Agencies reported that 9 percent of their systems were not categorized by risk level. The majority of systems without risk levels assigned were found at 4 agencies. One agency did not categorize 77 percent of its systems. Without assigned risk levels, agencies cannot make risk-based decisions on the security needs of their information and information systems.

Actions are Needed to Improve FISMA Reporting and Underlying Information Security Weaknesses

There are actions that OMB and the agencies can take to improve FISMA reporting and compliance and to address underlying weaknesses in information security controls. In our July 2005 report,[12] we evaluated the adequacy and effectiveness of agencies' information security policies and practices and the federal government's implementation of FISMA requirements. We recommended that the Director of OMB take actions in revising future FISMA reporting instructions to increase the usefulness of the agencies' annual reports to oversight bodies by:

- requiring agencies to report FISMA data by risk category;
- reviewing guidance to ensure the clarity of instructions;
- requesting the IGs report on the quality of additional agency processes, such as the annual system reviews.

[12]GAO-05-552

These recommendations were designed to strengthen reporting under FISMA by encouraging more complete information on the implementation of agencies' information security programs.

Consistent with our recommendation, OMB required agencies to report certain performance measures by system risk level for the first time in fiscal year 2005. As a result, we were able to identify potential areas of concern in the agencies' implementation of FISMA. For example, agencies do not appear to be prioritizing certain information security control activities, such as annual review of contractor systems or testing of contingency plans, based on system risk levels. For both of these activities, federal implementation of the control is lower for high-risk systems than it is for moderate or low-risk systems.

OMB has also taken steps to increase the clarity of instructions in their annual guidance. It has removed several questions from prior years that could have been subject to differing interpretations by the IGs and the agencies. Those questions related to agency inventories and to plans of actions and milestones. In addition, OMB clarified reporting instructions for minimally acceptable configuration requirements. The resulting reports are more consistent and, therefore, easier to analyze and compare.

However, opportunities still exist to enhance reporting on the quality of the agencies' information security-related processes. The qualitative assessments of the certification and accreditation process and the plans of actions and milestones have greatly enhanced Congress', OMB's, and our understanding of the implementation of these requirements at the agencies. Additional information on the quality of agencies' processes for annually reviewing or testing systems, for example, could improve understanding of these processes by examining whether federal guidance is applied correctly, or whether weaknesses discovered during the review or test are tracked for remediation. Extending qualitative assessments to additional agency processes could improve the information available on agency implementation of information security requirements.

Federal Agencies Need to Take Actions to Increase FISMA Compliance and Address Already Identified Information Security Weaknesses

Agencies need to take action to implement the information security management program mandated by FISMA and use that program to address their outstanding information security weaknesses. An agencywide security program provides a framework and continuing cycle of activities for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

As we have previously reported,[13] none of the 24 major agencies has fully implemented agencywide information security programs as required by FISMA. Agencies often did not adequately assess risks, develop sufficient risk-based policies or procedures for information security, ensure that existing policies and procedures were implemented effectively, or monitor operations to ensure compliance and determine the effectiveness of existing controls. Moreover, as demonstrated by the 2005 FISMA reports, many agencies still do not have complete and accurate inventories of their major systems. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded against unauthorized use, disclosure, and modification.

Agencies need to take action to implement and strengthen their information security management programs. Such actions should include completing and maintaining an accurate, complete inventory of major systems, and prioritizing information security efforts based on system risk levels. Strong incident procedures are necessary to detect, report, and respond to security incidents effectively.

[13] GAO-05-552.

Agencies also should implement strong remediation processes that include processes for planning, implementing, evaluating, and documenting remedial actions to address any identified information security weaknesses. Finally, agencies need to implement risk-based policies and procedures that efficiently and effectively reduce information security risks to an acceptable level.

Even as federal agencies are working to implement information security management programs, they continue to have significant control weaknesses in their computer systems that threaten the integrity, reliability, and availability of federal information and systems. In addition, these weaknesses place financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

The weaknesses appear in both access controls and other information security controls defined in our audit methodology for performing information security evaluations and audits.[14] These areas are (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) software change controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations, and (5) an agencywide security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

In the 24 major agencies' fiscal year 2005 reporting regarding their financial systems, 6 reported information security as a material

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

weakness and 14 reported it as a reportable condition.[15] Our audits also identified similar weaknesses in nonfinancial systems. In our prior reports, we have made specific recommendations to the agencies to mitigate identified information security weaknesses. The IGs have also made specific recommendations as part of their information security review work.

Agencies Should Address Weaknesses in Access Controls

Agencies would benefit from addressing common weaknesses in access controls. As we have previously reported, the majority of the 24 major agencies had access control weaknesses.[16] A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Based on our previous work performing information security audits, agencies can take steps to enhance the four basic areas of access controls:

- *User identification and authentication.* To enable a computer system to identify and differentiate users so that activities on the system can be linked to specific individuals, agencies assign unique user accounts to specific users, a process called identification. Authentication is the method or methods by which a system establishes the validity of a user's claimed identity. Agencies need to implement strong user identification and authentication controls.
- *User access rights and file permissions.* The concept of "least privileged" is a basic underlying principle for security computer systems and data. It means that users are only granted those access rights and file permissions that they need to do their work. Agencies would benefit from establishing the concept of least privilege as the basis for all user rights and permissions.
- *Network services and devices.* Sensitive programs and information are stored on networks, which are collections of interconnected

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

[16]GAO-05-552.

computer systems and devices that allow users to share resources. Organizations secure their networks, in part, by installing and configuring networks devices that permit authorized requests and limit services that are available.[17] Agencies need to put in place strong controls that ensure only authorized access to their networks.

- *Audit and monitoring of security-related events*. To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial that agencies implement system or security software that provides an audit trail that they can use to determine the source of a transaction, or to monitor the activities of users on the agencies' systems. To detect and prevent unauthorized activity, agencies should have strong monitoring and auditing capabilities.

Agencies Need to Act to Implement Other Information Security Controls

In addition to electronic access controls, other important controls should be in place to ensure the security and reliability of an agency's data.

- *Software change controls.* Counteracting identified weaknesses in software change controls would help agencies ensure that software was updated correctly and that changes to computer systems were properly approved. Software change controls ensure that only authorized and fully tested software is placed in operation. These controls -- which also limit and monitor access to powerful programs and sensitive files associated with computer operations -- are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. These policies, procedures, and techniques help to ensure that all programs and program modifications are properly authorized, tested, and approved. Failure to implement these controls increases the risk that unauthorized programs or changes could be -- inadvertently or deliberately -- placed into operation.

[17]Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network; (2) routers that filter and forward data; (3) switches that forward information through segments of a network; and, (4) servers that host applications and data.

- *Segregation of duties.* Agencies have opportunities to implement effective segregation of duties to address the weaknesses identified in this area. Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records. Proper segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. For example, agencies need to segregate duties to ensure that individuals cannot add fictitious users to a system, assign them elevated access privileges, and perform unauthorized activities without detection. Without adequate segregation of duties, there is an increased risk that erroneous or fraudulent transactions can be processed, improper program changes implemented, and computer resources damaged or destroyed.
- *Continuity of operations.* The majority of agencies could benefit from having adequate continuity of operations planning. An organization must take steps to ensure that it is adequately prepared to cope with the loss of operational capabilities due to earthquake, fire, accident, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity of operations plan. To ensure that the plan is complete and fully understood by all key staff, it should be tested, including surprise tests, and test plans and results documented to provide a basis for improvement. Among the aspects of continuity planning that agencies need to address should be: (1) ensuring that plans contain adequate contact information for emergency communications; (2) documenting the location of all vital records for the agencies and methods of updating those records in an emergency; (3) conducting tests, training, or exercises frequently enough to have assurance that the plan would work in an emergency. Losing the capability to process, retrieve, and protect information that is maintained electronically can significantly affect an agency's ability to accomplish its mission.
- *Physical security.* Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed. With inadequate

physical security, there is increased risk that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

In summary, through the continued emphasis of information security by Congress, the administration, agency management, and the accountability community, the federal government has seen improvements in its information security. However, despite the advances shown by increases in key performance measures, progress remains mixed. If information security is to continue to improve, agency management must remain committed to the implementation of FISMA and the information security management program it mandates. Only through the development of strong IT security management can the agencies address the persistent, long-standing weaknesses they face in information security controls.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the Committee may have at this time. Should you have any questions about this testimony, please contact me at (202) 512-6244. I can also be reached by e-mail at wilshuseng@gao.gov. Individuals making key contributions to this testimony include Suzanne Lightman, Assistant Director, Larry Crosland, Joanne Fiorino, and Mary Marshall.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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