United States Government Accountability Office

GAO

Testimony

Before the House Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security

For Release on Delivery
2:00 p.m. EDT
Thursday, April 14, 2005

INFORMATION SECURITY

Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues

April 14, 2005

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-567T, a testimony before the House Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security

INFORMATION SECURITY

Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements

Why GAO Did This Study

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

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made 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. FISMA requires that agencies report annually to OMB who issues guidance for that reporting process.

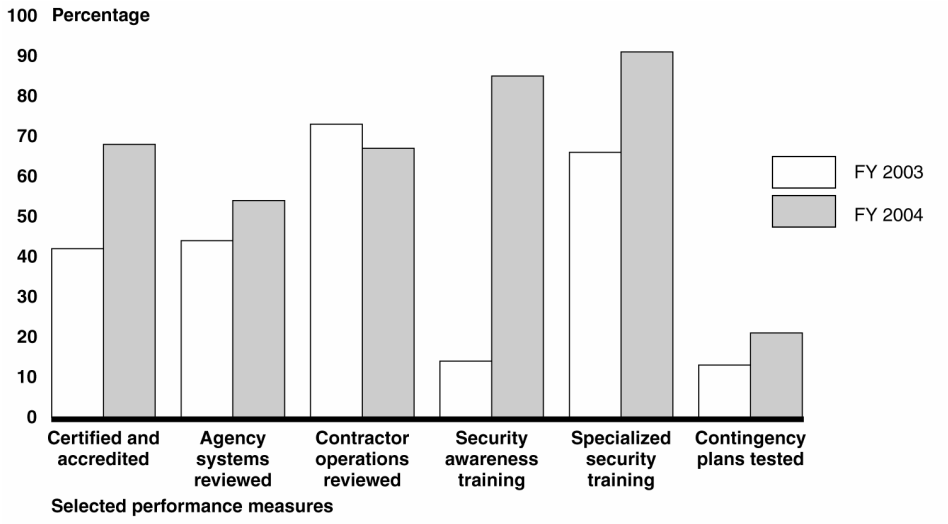
The Department of Homeland Security (DHS), the third largest agency in the federal government, uses a variety of major applications and general systems in support of operational and administrative requirements.

This testimony discusses DHS's progress and challenges in implementing FISMA as reported by the agency and its Inspector General (IG).

What GAO Found

DHS has made progress in implementing key federal information security requirements, yet it continues to face challenges in fulfilling the requirements mandated by FISMA. In its fiscal year 2004 report on FISMA implementation, DHS highlights increases in the majority of the key performance measures (developed by the Office of Management and Budget (OMB) to track agency performance in implementing information security requirements), such as the percentage of agency systems reviewed and percentage of employee and contractor personnel who received security awareness training (see figure). For example, DHS reported a substantial increase in the percentage of personnel that received security awareness training, rising from 14 percent in fiscal year 2003 to 85 percent in fiscal year 2004. However, DHS continues to face significant challenges in meeting most statutory information security requirements. For example, DHS has yet to develop a complete and accurate inventory or an effective remediation process.

Figure: DHS Performance Data for Key OMB Performance Measures



Sources: DHS' FY2003 and FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

www.gao.gov/cgi-bin/getrpt?GAO-05-567T.

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

Abbreviations

CIO	chief information officer
DHS	Department of Homeland Security
DOD	Department of Defense
FISMA	Federal Information Security Management Act of 2002
IG	inspector general
IT	information technology
OMB	Office of Management and Budget
NIST	National Institute of Standards and Technology

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts by the Department of Homeland Security (DHS) 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] Accordingly, since 1997, we have identified information security as a governmentwide high-risk issue in reports to Congress—most recently in January 2005.[3] Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made them vulnerable to attack, Congress passed FISMA, which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies. Under FISMA, agencies are to report annually to the Office of Management and Budget (OMB) who issues guidance for that reporting.

In my testimony today, I will summarize the reported status of DHS's implementation of FISMA, including areas of progress and continuing challenges.

In conducting this review, we analyzed and summarized DHS's fiscal year 2003 and 2004 reports to Congress on FISMA implementation. We also reviewed and summarized the fiscal year 2004 FISMA reports for 24 of the largest federal agencies and their Inspectors General (IGs). In addition, we reviewed standards and guidance issued by Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) pursuant to their FISMA responsibilities. Finally, we reviewed OMB's 2004 report to

[1] *Federal Information Security Management Act of 2002*, *Title III*, *E-Government Act of 2002*, Pub. L. No. 107-347, December 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.: January, 2005).

Congress on the implementation of FISMA governmentwide.[4] We did not validate the accuracy of the data reported by DHS, the other 23 CFO agencies, or OMB, but did analyze the IGs' fiscal year 2004 FISMA reports to identify any issues related to the accuracy of agency-reported information. We performed our work from October 2004 to March 2005 in accordance with generally accepted government auditing standards. In addition, we continue to perform on-going work on DHS's management of information security.

Results in Brief

DHS has made progress in implementing key federal information security requirements, yet it continues to face challenges in fulfilling the requirements mandated by FISMA. In its fiscal year 2004 report on FISMA implementation, DHS highlights increases in the majority of the key performance measures (developed by OMB to track agency performance in implementing information security requirements), such as the percentage of agency systems reviewed and percentage of employee and contractor personnel who received security awareness training. For example, DHS reported a substantial increase in the percentage of personnel that received security awareness training, rising from 14 percent in fiscal year 2003 to 85 percent in fiscal year 2004. However, DHS continues to face significant challenges in meeting most statutory information security requirements. For example, DHS has yet to develop a complete and accurate inventory or an effective remediation process.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world

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

communicate and conduct business. While the benefits have been enormous, without proper safeguards, this widespread interconnectivity also poses significant risks to the government's computer systems and, more importantly, to the critical operations and infrastructures they support.

We recently reported that, while federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses in federal computer systems that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at the risk of disruption. The significance of these weaknesses led us to conclude in the audit of the federal government's fiscal year 2004 financial statements[5] that information security was a material weakness.[6] Our audits also identified instances of similar types of weaknesses in non-financial systems. Weaknesses continued to be reported in each of the six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

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

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

[6]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.

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

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

FISMA Authorized and Strengthened Information Security Requirements

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

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

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

FISMA also established a requirement that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or that are under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

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

national security systems are to be performed only by an entity designated by the agency head.

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

Other major provisions require NIST to develop, for systems other than national security systems: (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST must also develop a definition and guidelines concerning detection and handling of information security incidents and guidelines, developed in conjunction with the Department of Defense (DOD) and the National Security Agency, for identifying an information system as a national security system.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

Consistent with FISMA requirements, OMB issues guidance to the agencies on their annual reporting requirements. On August 23, 2004, OMB issued its fiscal year 2004 reporting instructions. The reporting instructions, similar to the 2003 instructions, emphasized a strong focus on performance measures and formatted these instructions to emphasize a quantitative response. OMB has developed performance measures in the following areas, including:

- certification and accreditation,[7]
- annual review of agency systems,
- annual review of contractor operations or facilities,
- annual security awareness training for employees and contractors,
- annual specialized training for employees with significant security responsibilities, and
- testing of contingency plans.

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

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

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

evaluations of a subset of agency systems, IGs were asked to assess the reliability of the data for those systems that they evaluated.

Recently-created Department of Homeland Security is Large and Complex

In the aftermath of September 11, invigorating the nation's homeland security missions became one of the federal government's most significant challenges. The Homeland Security Act of 2002 created DHS, combining 22 agencies into one department. DHS, with an estimated 170,000 employees, is the third largest government agency. Not since the creation of DOD more than 50 years ago had the government sought an integration and transformation of this magnitude.

GAO designated implementing and transforming DHS as high risk in 2003 because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to effectively address its management challenges and program risks could have serious consequences for our national security.[8] DHS combined 22 agencies specializing in various disciplines: law enforcement, border security, biological research, disaster mitigation, and computer security, for instance. Further, DHS oversees a number of non-homeland-security activities, such as the Coast Guard's marine safety responsibilities and the Federal Emergency Management Agency's natural disaster response functions.

DHS has lead responsibility for preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing the damage and assisting in the recovery from attacks that do occur. DHS has five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness

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

and response. In addition, the department has four other organizations that report directly to the Secretary.

DHS uses a variety of major applications and general support systems in support of operational and administrative requirements. In its 2004 FISMA report, DHS stated that it had 395 systems and 61 contractor operations. These systems often served specific organizations that are now merged with others, resulting in interoperability issues, data management concerns, and incompatible environments or duplicative processes.

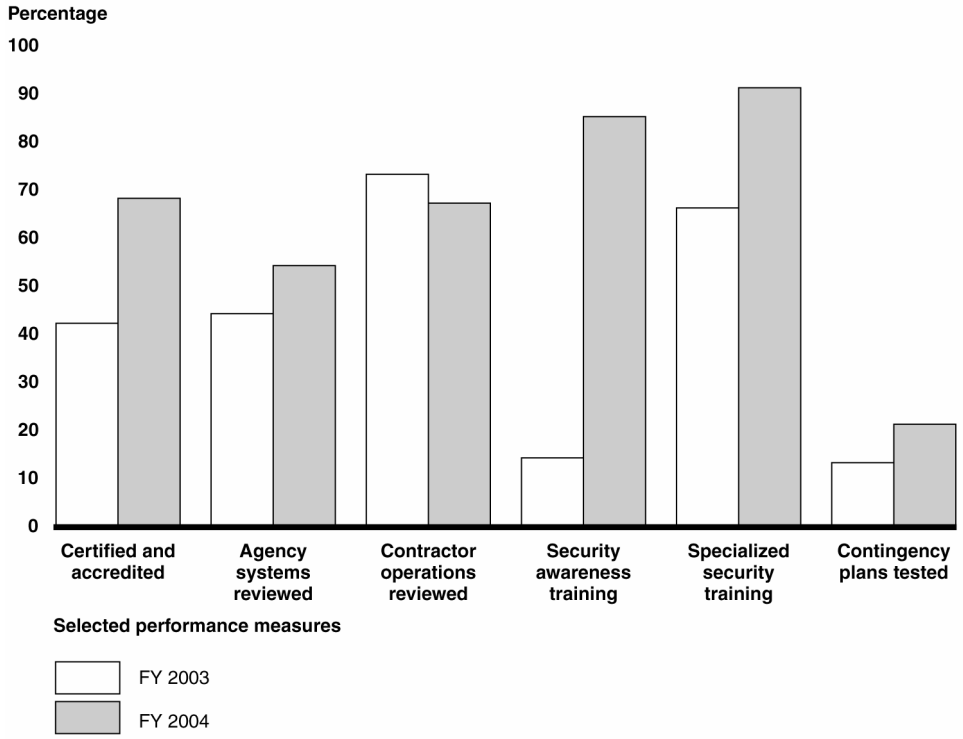
Department of Homeland Security's FISMA Reports Highlight Increases in Performance Measures, but Challenges Remain

In its FISMA-mandated report for fiscal year 2004, DHS generally reported increases in compliance with information security requirements as compared with 2003. However, DHS continues to face significant challenges. The following key performance measures showed increased performance and/or continuing challenges:

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

Figure 1 illustrates the reported overall status of DHS in meeting these performance measures and the changes between fiscal years 2003 and 2004.

Figure 1: DHS Reported Data for Key Performance Measures

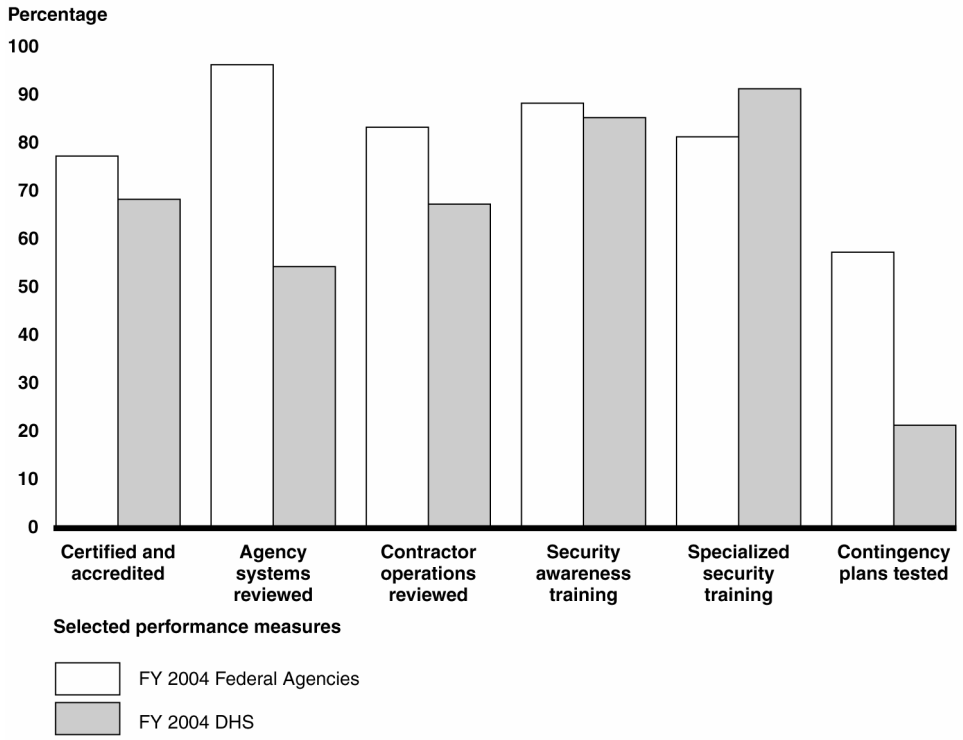


Sources: DHS' FY2003 and FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

DHS has yet to develop a complete and accurate inventory, or an effective plan of action and milestones.[9] Finally, figure 2 illustrates how DHS compares to the governmentwide results for the performance measures when compared to the aggregated data of all 24 CFO agencies.

[9]OMB's implementing guidance refers to the process of planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security as a security plan of action and milestones.

Figure 2: Comparison of DHS Data to Governmentwide Performance



Sources: OMB's FY2004 Report to Congress on the Federal Information Security Management Act and DHS' FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

Certification and Accreditation

Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. In 2003, agencies were required to report separately on risk assessments and security plans. In 2004, OMB eliminated this separate reporting in its guidance and directed agencies to complete risk assessments and security plans for the certification and accreditation process to be accomplished. As a result, the performance measure for certification and accreditation now also

reflects the level of agency compliance for risk assessments and security plans. For FISMA reporting, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation.

DHS reported a significant increase for this performance measure in its fiscal year 2004 report. The Department reported that approximately 68 percent of its systems had been certified and accredited, an increase of 26 percent over fiscal year 2003. Governmentwide, 77 percent of all systems were certified and accredited compared to the 68 percent at DHS. If agencies do not certify and accredit their systems, they cannot be assured that risks have been identified and mitigated to an acceptable level.

Moreover, the DHS IG reported in its 2004 FISMA report that the certification and accreditation process at the Department was poor. The report noted that the certification and accreditation process was not performed consistently across the Department. In addition, there were instances where certified and accredited systems lacked key security documentation such as up-to-date and approved security plans, a current risk assessment, and contingency plans. As a result, the agency reported performance data may not accurately reflect the status of DHS's efforts to implement this requirement.

Annual Review of Agency Systems

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

considered along with control testing and evaluation in IG and GAO audits to help provide a more complete picture of the agencies' security postures. As a performance measure for this requirement, OMB requires that agencies report the number of systems that they have reviewed during the year.

DHS reported performing an annual review on an increased percentage of its systems. It reported in 2004 that it had reviewed 54 percent of its systems, as compared to 44 percent in 2003. In 2004, 23 of the 24 CFO agencies reported that they had reviewed 90 percent or more of their systems. Annual security testing helps to provide assurance to the agencies that security controls are in place and functioning correctly. Without such testing, agencies cannot be assured that their information and systems are protected.

Annual Review of Contractor Operations

Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. Thus, agency information 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. Other such organizations may include contractors, grantees, state and local governments, and industry partners. This underscores longstanding OMB policy concerning sharing government information and interconnecting systems: federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

At DHS, the key performance measure of annually reviewing contractor operations showed a minor decrease from 73 percent in 2003 to 67 percent in 2004. Twenty of the Department's contractor operations were not reviewed. The governmentwide performance measure was reported as 83 percent of all contractor operations reviewed. If agencies do not review contractor operations, they cannot be assured that federal data is being handled in accordance with agency requirements.

Security Awareness Training

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading organizations[10] 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. Agencies reported that they provided security awareness training to the majority of their employees and contractors. As performance measures for FISMA training requirements, OMB has the agencies report the number of employees and contractors who received IT security training during fiscal year 2004.

DHS reported a substantial increase in the percentage of employees and contractors who received security awareness training in fiscal year 2004. The Department reported that it had trained 85 percent of its staff compared to 14 percent in 2003. As a result, reported performance is comparable to the majority of agencies in this performance measure, as seventeen agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness.

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 updated on changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. OMB directs

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

agencies to report on the percentage of their employees with significant security responsibilities who received specialized training.

DHS presented substantial improvement in this performance measure, reporting that it had provided specialized training to more than 90 percent of its employees who have significant security responsibilities. Not only was this a significant improvement over the 66 percent reported in 2003, it also places DHS among the top ten agencies governmentwide for this performance measure. Given the rapidly changing threats in information security, agencies need to keep their IT security employees up-to-date on changes in technology. Otherwise, agencies may face increased risk of security breaches.

Testing of Contingency Plans

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

The testing of contingency plans is essential to determining whether plans will function as intended in an emergency situation. The frequency of plan testing will vary depending on the criticality of the entity's operations. The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. To show the status of implementing this requirement, OMB requires that agencies report

the number of systems that have a contingency plan and the number that have contingency plans that have been tested.

DHS reported a modest increase in the percentage of contingency plans tested. The department stated that it had tested contingency plans for 21 percent of its systems, an 8 percentage point increase over 2003. Moreover, analysis of the numbers reveals that DHS tested 82 plans, which was almost double what it tested in 2003. However, the majority of its systems do not have tested contingency plans. Overall, federal agencies reported that 57 percent of systems had contingency plans that had been tested. Without testing, agencies can have limited assurance that they will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption.

Other Challenges in Implementing Statutory Requirements

In addition to the performance measures, there are other requirements that agencies must meet under FISMA. Agencies are required to have a complete and accurate inventory of their major systems and any interdependencies. They are also required to have a remediation process for correcting identified information security weaknesses.

The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. Further, a complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources.

DHS reported that it did not have a complete and accurate inventory in either 2003 or 2004. Without reliable information on DHS's inventories, the Department, the administration, and Congress cannot be fully assured of DHS's progress in implementing FISMA.

FISMA requires each agency to develop a process for planning, implementing, evaluating, and documenting remedial actions to

address any deficiencies in the information security policies, procedures and practices of the agency. OMB's implementing guidance refers to this process as a security plan of action and milestones. The chief information officer (CIO) is to manage the process for the agencies and program officials are required to regularly update the CIO on their progress in implementing remedial actions. This process allows both the CIO and the IG to monitor agency-wide progress, identify problems, and provide accurate reporting. In its annual reporting guidance, OMB asks the agency IGs to report on the status of the plan of action and milestones at their agencies. IGs were asked to evaluate the process based on the following criteria:

- known IT security weaknesses from all components are incorporated;
- program officials develop, implement and manage plans for the systems they own and operate that have an IT security weakness;
- program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress;
- CIO develops, implements and manages plans for the systems they own and operate that have an IT security weakness;
- CIO centrally tracks, maintains, and reviews all plan activities on at least a quarterly basis;
- The plan is the authoritative agency tool for agency and IG management to identify and monitor agency actions for corrected information security weaknesses;
- System-level plans are tied directly to the system budget request through the IT business case as required in OMB budget guidance;
- IG has access to the plans as requested;
- IG findings are incorporated into the process; and
- the process prioritizes IT security weaknesses to help ensure that significant weaknesses are addressed in a timely manner and receive appropriate resources.

In its 2004 FISMA report, the DHS IG described problems with the plan of action and milestones process at DHS. According to the IG, seven of the nine major department components reviewed lacked a

documented and implemented plan of action and milestones. Further, the IG stated that the CIO did not receive reports of remediation progress and did not ensure that components updated the status of their progress. Linkage of the plans to budget requests was reported as minimal at the component level. Seven of the nine components reviewed did not have a formal process to prioritize their IT security weaknesses. Finally, the IG reported that its findings were not incorporated into the plan of action and milestones at DHS. Without an effective, implemented remediation process, DHS cannot be assured that identified security weaknesses are tracked and corrected.

In summary, DHS generally showed increases in the OMB performance measures for FISMA implementation in fiscal year 2004. However, it still faces challenges in implementing the statutory requirements. It faces significant challenges in both inventory development and the implementation of its remediation process. Accordingly, if information security is to continue to improve, agency management must remain committed to these efforts. The annual reports and performance measures will continue to be key tools for holding DHS accountable and providing a barometer of the overall status of its information security.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions from you or members of the Committee.

Should you have any questions about this testimony, please contact me at (202) 512-3317 or Suzanne Lightman, Assistant Director, at (202) 512-8146 or by e-mail at wilshuseng@gao.gov and lightmans@gao.gov, respectively.

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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