United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

October 2006

# INFORMATION SECURITY

# Agencies Need to Develop and Implement Adequate Policies for Periodic Testing


GAO-07-65

October 2006

# INFORMATION SECURITY

# Agencies Need to Develop and Implement Adequate Policies for Periodic Testing

GAO Accountability · Integrity · Reliability

## Highlights

Highlights of GAO-07-65, a report to the Chairman, Committee on Government Reform, House of Representatives

## Why GAO Did This Study

Agencies rely extensively on computerized information systems and electronic data to carry out their missions. To ensure the security of the information and information systems that support critical operations and infrastructure, federal law and policy require agencies to periodically test and evaluate the effectiveness of their information security controls at least annually.

GAO was asked to evaluate the extent to which agencies have adequately designed and effectively implemented policies for testing and evaluating their information security controls.

GAO surveyed 24 major federal agencies and analyzed their policies to determine whether the policies address important elements for periodic testing. GAO also examined testing documentation at 6 agencies to assess the quality and effectiveness of testing on 30 systems.

## What GAO Recommends

This report contains recommendations to strengthen governmentwide guidance and reporting on agencies' periodic testing of information security controls. OMB said it would consider GAO's recommendations. The Department of Commerce stated that the National Institute of Standards and Technology is reviewing its guidance to assist agencies in strengthening their programs.

www.gao.gov/cgi-bin/getrpt?GAO-07-65.

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

Federal agencies have not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Agencies' policies often did not include important elements for performing effective testing. For example, none of the agencies' policies addressed how to determine the depth and breadth of testing according to risk. Also, agencies did not always address other important elements, including the identification and testing of security controls common to multiple systems, the definition of roles and responsibilities of personnel performing tests, and the frequency of periodic testing.

The six case study agencies did not effectively implement policies for periodically testing and evaluating information security controls for the 30 systems reviewed. The methods and practices for testing and evaluating controls at the six agencies were not adequate to ensure that assessments were consistent, of similar quality, and repeatable. For example, these agencies did not always sufficiently document their test methods and results, did not define the assessment methods to be used when evaluating security controls, did not test security controls as prescribed, and did not include previously reported remedial actions or weaknesses in their test plans to ensure they had been addressed (see table). As a result, agencies may not have reasonable assurance that controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

**Systems with Testing Weaknesses**

| Insufficient testing documentation | Inadequately defined assessment method | Inadequate test of security control | Inadequately documented remedial actions in test plans |
|---|---|---|---|
| 28 | 7 | 24 | 18 |

Source: GAO analysis of agency FY 2005 test results (management, operational, and technical controls) and test documentation.

# Contents

## Abbreviations

| | |
|---|---|
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act of 2002 |
| OMB | Office of Management and Budget |
| NIST | National Institute of Standards and Technology |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

October 20, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives

Dear Mr. Chairman:

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems through 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 (FISMA) in 2002.[1]

Among other things, FISMA requires federal agencies to periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of developing and implementing an agencywide information security program. In addition, agencies and their Inspectors General are required to annually report to Congress and the Office of Management and Budget (OMB) on the adequacy and effectiveness of information security policies and practices and compliance with the act. The act also assigns specific responsibilities to OMB and the National Institute of Standards and Technology (NIST). OMB's responsibilities include (1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and (2) reporting to Congress on the agencies' compliance with FISMA requirements. OMB also provides instructions to agencies and Inspectors General to assist them in meeting FISMA reporting requirements. These instructions have a strong focus on performance measures, which are the basis of agencies' annual reports and Inspectors General independent annual evaluations. The act requires

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

NIST to develop, for systems other than national security systems,[2] standards and guidelines to assist agencies in implementing their information security programs.

As agreed with your office, our objective was to determine whether agencies have adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. To accomplish this objective, we conducted a survey of 24 major federal agencies[3] and their Inspectors General, analyzed information security policies, and selected 6 of the 24 agencies to use as case studies for conducting in-depth evaluations of their periodic testing and evaluation methods and practices. Specifically, to determine whether the 24 agencies adequately designed policies for periodic testing, we obtained and analyzed their policies to determine whether they included elements important for conducting effective tests and evaluations. To determine whether the 6 agencies had effectively implemented policies and procedures, we assessed methods and practices used to test and evaluate controls for 30 of their systems. We examined instructions, standards, and guidelines issued by OMB and NIST as a framework for assessing the adequacy of the 24 agencies' policies and for determining the effectiveness of the 6 agencies' testing and evaluation methods and practices. Details of our objective, scope, and methodology are included in appendix I.

We conducted our work from November 2005 through July 2006 in accordance with generally accepted government auditing standards.

[2]As defined in FISMA, the term "national security systems" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency (1) the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

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

## Results in Brief

Agencies have not adequately designed and effectively implemented policies for performing periodic testing and evaluation of information security controls. Agencies' policies often did not include elements important for performing effective testing. For example, none of the agencies' policies addressed how to determine the depth and breadth of testing according to risk. Also, agencies did not always address other important elements, including the identification and testing of security controls common to multiple systems, the definition of roles and responsibilities of personnel performing tests, and the frequency of their periodic testing.

The six case study agencies did not effectively implement policies for periodically testing and evaluating information security controls for the 30 systems we reviewed. The methods and practices for testing and evaluating controls at the six agencies were not adequate to provide reasonable assurance that assessments were consistent, of similar quality, and repeatable. For example, these agencies did not always have sufficient documentation to support testing methods and results, did not define the assessment methods to be used when evaluating security controls, and did not include remedial actions in testing plans.

As a result, agencies do not have reasonable assurance that controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

We are recommending that the Director of OMB instruct agencies to develop and implement policies on periodic testing and evaluations and revise instructions for future FISMA reporting by requesting Inspectors General to report on the quality of agencies' periodic testing processes. We are also recommending that the Secretary of the Department of Commerce direct the Director of NIST to strengthen guidance on determining the depth and breadth of testing security controls.

In oral comments on a draft of this report, OMB representatives from its Offices of Information and Regulatory Affairs and General Counsel agreed to consider our recommendations. We also received written comments from the Office of the Deputy Secretary of the Department of Commerce. He stated that NIST is already addressing our concerns and reviewing its guidance including depth and breadth of testing security controls (see app. II).

## 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 have also continued to have significant control weaknesses in federal computer systems, which puts federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.[4]

## Federal Law and Policy Establish Federal Information Security Testing Requirements

The Federal Information Security Management Act of 2002 requires each agency 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. Among other things, the program is to include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. The testing is to include management, operational, and technical controls for every system identified in the agency's required inventory of major information systems.

The act also assigns specific responsibilities to OMB and NIST. OMB's responsibilities include the following:

- Overseeing agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security.
- Reviewing agency information security programs, at least annually.

[4]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).

- Reporting to Congress annually on agency compliance with FISMA requirements.

  As part of the reporting process, OMB provides instructions[5] to agencies and their Inspectors General on the annual FISMA reporting requirements. These instructions include performance measures for such things as the number of systems for which security controls have been tested and evaluated in the past year. OMB also uses performance measures to assist in its oversight responsibilities and to annually report to Congress on agencies' compliance with the requirements of the act.

  FISMA also directs NIST to develop standards and guidelines for systems other than national security systems. These standards and guidelines instruct agencies on providing an acceptable level of information security for all agency operations and assets and contribute to the testing and evaluation of information security controls within an agencywide information security program. Recognizing the importance of documenting standards and guidelines as part of an agencywide information security program, NIST emphasizes that agencies must develop and promulgate formal, documented policies and procedures in order to ensure the effective implementation of security requirements.

  NIST standards and guidelines that contain elements applicable to periodic testing and evaluation include the following:

- Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001. This publication is a self-assessment guide for agencies to use in determining the current status of their information security program. The guide includes a standardized form for reporting the results of system-level assessments and a method for evaluating the effectiveness of the agency's information security program. The guide also emphasizes the importance of establishing levels of implementation, referred to as the IT security assessment framework. NIST Special Publication 800-26 is effective through the 2006 FISMA

[5]OMB, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-06-20 (Washington, D.C.: July 17, 2006).

reporting period and will be rescinded when Special Publications 800-53A and 800-100[6] are finalized.

- Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004. This guide is to be used for certifying and accrediting nonnational security systems. Developed as part of NIST's project to promote the development of standards and guidelines to support FISMA, this guide specifies the need for ongoing activities to continuously monitor the effectiveness of security controls.

- Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005. This publication provides instructions on selecting and specifying security controls for information systems. It also provides the set of security controls that satisfy the depth and breadth of security requirements levied on information systems and provides the fundamental concepts associated with security controls selection and specification, including the identification and use of common security controls. In conducting security assessments, NIST states that assessment results[7] can be used and shared to enhance the efficiency of evaluations and reduce security program costs.

- Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, April 2006. The publication is a second public draft to be used by agencies to assess the effectiveness of security controls employed in federal information systems. NIST establishes methods and procedures to assess the security controls in federal information systems, specifically those controls listed in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. These methods and procedures are designed for agencies to use in determining if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to

[6]NIST Special Publication 800-100 (draft) provides a broad overview of information security program elements that inform members of the information security management team how to establish and implement an information security program. The handbook summarizes and augments a number of existing NIST standards and guidance documents and provides additional information on related topics.

[7]Security control assessment results can come from a number of sources, such as certifications conducted as part of a routine information system accreditation or reaccreditation process, ongoing continuous monitoring activities, self-assessments, or routine testing and evaluation of the information system as part of the ongoing system development life-cycle process.

meeting the security requirements of the agency. NIST closed acceptance of public comments on this draft on July 31, 2006, and plans to issue a final publication in December 2006.

## Elements Important for Performing Effective Testing and Evaluation

Having well-designed policies is critical for performing effective testing and evaluation of security controls. To assist agencies, OMB and NIST developed instructions, standards, and guidelines for testing and evaluating the controls over information systems. We used the following six elements to evaluate agencies' policies for periodically testing security controls:

1. Identifying the frequency of periodic testing.
2. Defining roles and responsibilities of personnel performing the testing.
3. Selecting a minimum set of security controls evaluated during periodic tests.
4. Identifying and testing common security controls.
5. Determining the depth and breadth of periodic testing.
6. Including assessment results in remediation plans.

The related federal and NIST references are shown in table 1.

**Table 1: Elements for Performing Testing and Evaluation and References to Related Federal Standards and Guidelines**

| Element | Description | Federal references |
|---|---|---|
| 1. Identifying frequency of periodic testing | FISMA requires each agency to perform for all systems in their inventory "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually." | FISMA<br>OMB Memorandum M-05-15<br>OMB Memorandum M-06-20<br>NIST Special Publication 800-37<br>NIST Special Publication 800-53<br>NIST Special Publication 800-53A (second draft) |
| 2. Defining roles and responsibilities | Agencies must ensure that the appropriate officials are assigned roles and responsibilities for testing and evaluating controls over systems. | OMB Memorandum M-05-15<br>OMB Memorandum M-06-20<br>NIST Special Publication 800-26<br>NIST Special Publication 800-37<br>NIST Special Publication 800-53A (second draft) |

| Element | Description | Federal references |
|---|---|---|
| 3. Selecting minimum security controls evaluated during periodic tests | Once agencies have categorized their information and information systems according to the impact level, they must select an appropriate set of controls (baseline) that satisfy the minimum requirements necessary to achieve adequate security. These controls are assessed using appropriate methods and procedures. | FISMA<br>FIPS Publication 199<br>FIPS Publication 200<br>NIST Special Publication 800-26<br>NIST Special Publication 800-37<br>NIST Special Publication 800-53<br>NIST Special Publication 800-53A (second draft) |
| 4. Identifying and testing common security controls | Agencies should adopt an organizationwide view of an information security program by identifying common security controls that can be applied to one or more information systems so they can achieve efficiencies by testing common controls and using the results for multiple systems. | NIST Special Publication 800-37<br>NIST Special Publication 800-53<br>NIST Special Publication 800-53A |
| 5. Determining the depth and breadth of periodic testing | Agencies should consider the appropriate depth and breadth of periodic testing based on the potential risk and magnitude of harm, the relative comprehensiveness of prior reviews, and the adequacy and successful implementation of the remediation plans for weaknesses in the systems so they can take advantage of testing methodologies and assessments to achieve cost efficiencies. | OMB Memorandum M-05-15<br>OMB Memorandum M-06-20<br>NIST Special Publication 800-37<br>NIST Special Publication 800-53<br>NIST Special Publication 800-53A (second draft) |
| 6. Including assessment results in remediation plans | Agencies' assessment results and findings should be reviewed and included in the remediation plans to ensure that identified deficiencies in the information security policies, procedures, and practices are remedied. | OMB Memorandum M-05-15<br>OMB Memorandum M-06-20<br>NIST Special Publication 800-26<br>NIST Special Publication 800-37<br>NIST Special Publication 800-53A (second draft) |

Source: GAO analysis of federal law and guidelines.

## Agencies' Policies Do Not Fully Address Elements Important for Effective Testing and Evaluation

Agencies' policies for periodically testing and evaluating security controls have not been adequately designed and effectively implemented. Specifically, none of the federal agencies' policies fully addressed six important elements included in OMB and NIST guidelines and standards for performing effective security testing and evaluations. In addition, there were weaknesses in the security control assessments for the 30 systems reviewed at the six case study agencies. As a result, agencies have limited assurance that controls are implemented correctly, operating as intended, and producing the desired outcome. In addition, agencies may not be fully aware of security control weaknesses in their systems, thereby leaving the agencies' operations and systems at risk.

## Agencies' Policies Have Design Weaknesses

Agencies did not fully address six elements important for testing and evaluating security controls in their policies. Specifically, the (1) frequency of periodic testing was not always identified, (2) roles and responsibilities of personnel performing tests often were not clearly defined, (3) selection of a minimum set of security controls evaluated during periodic tests was not always fully addressed, (4) instructions on identification and testing of common security controls were not addressed, (5) instructions on determining the depth and breadth of testing were not included, and (6) descriptions of a process for documenting remedial actions to address deficiencies were not always addressed. Table 2 indicates weaknesses in developing and promulgating formal, documented policies to address the security elements needed for effective testing.

**Table 2: Weaknesses in 24 Federal Agencies' Policies by Element**

| | Elements for periodically testing and evaluating security controls | | | | | |
|---|---|---|---|---|---|---|
| **Agency** | **Identify the frequency of periodic testing?** | **Define roles and responsibilities?** | **Provide instructions for selecting minimum security controls evaluated during periodic tests?** | **Specify the identification and testing of common security controls?** | **Instructions on determining the depth and breadth of testing?** | **Describe a process for documenting weaknesses in remediation plans?** |
| Agency 1 | | X | | X | X | X |
| Agency 2[a] | No policies | No policies | No policies | No policies | No policies | No policies |
| Agency 3 | | | | X | X | |
| Agency 4 | | X | X | X | X | X |
| Agency 5 | | X | | X | X | X |
| Agency 6 | | | X | X | X | |
| Agency 7 | X | X | X | X | X | |
| Agency 8 | | X | | X | X | X |
| Agency 9 | | | | X | X | |
| Agency 10 | | X | | X | X | |
| Agency 11 | | | | X | X | |
| Agency 12 | | X | X | X | X | |
| Agency 13 | | | X | X | X | |
| Agency 14 | X | X | X | X | X | |
| Agency 15 | | | X | X | X | X |
| Agency 16 | X | | | X | X | |
| Agency 17 | | X | X | X | X | X |
| Agency 18 | X | X | X | X | X | X |

| | Elements for periodically testing and evaluating security controls | | | | | |
|---|---|---|---|---|---|---|
| Agency | Identify the frequency of periodic testing? | Define roles and responsibilities? | Identify the frequency of periodic testing? | Specify the identification and testing of common security controls? | Identify the frequency of periodic testing? | Describe a process for documenting weaknesses in remediation plans? |
| Agency 19 | | X | | | X | |
| Agency 20 | | X | | X | X | X |
| Agency 21 | X | X | | X | X | |
| Agency 22 | X | X | X | X | X | |
| Agency 23 | | | X | X | X | X |
| Agency 24 | X | X | | X | X | X |
| **Total** | **7** | **15** | **11** | **22** | **23** | **10** |

Source: GAO analysis of agency policies (as of February 2006).

Note: "X" indicates weaknesses.

[a]The agency reported it did not have agencywide or component-level policy or guidance that addressed system security testing. However, the agency reported that a departmental manual on FISMA was under development.

## Policies Did Not Identify Frequency of Periodic Testing

FISMA requires agencies to perform—for all major information systems in their inventory—periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually.

Of the 23 agencies' policies we reviewed, 7 agencies did not require that their security controls (management, operational, and technical) be tested and evaluated at least annually. For example, policies for 3 of the 7 agencies did not specify the frequency of periodic testing. The other 4 agencies identified the frequency of some testing activities—reviewing the overall security program annually, testing standard user account procedures annually, and certifying and accrediting systems at least every 3 years[8]—but did not specify the frequency of periodic testing for other management, operational, and technical security controls. Unless agencies specify the frequency for conducting periodic testing and evaluations at least annually per FISMA, they may not have assurance that controls are being sufficiently evaluated and producing the desired outcome with respect to meeting the security requirements of the agency.

[8]Agencies are required to reaccredit their systems prior to a significant change in processing, but at least every 3 years (more often where there is a high risk and potential magnitude of harm).

## Policies Did Not Clearly Define Roles and Responsibilities for Periodic Testing

NIST 800-37 identifies the roles and associated responsibilities with regard to testing and evaluating information security controls. These roles include the chief information officer, authorizing official, senior agency information security officer, information system owner, and information system security officer. In addition, NIST Special Publication 800-26 specifies that agencies should have procedures in place that identify who is conducting the security testing.

Roles and responsibilities of personnel performing testing were not clearly defined in policies for 15 of the 23 agencies. Ten of the 15 agencies did not define roles and responsibilities for personnel performing tests in their policies and the other 5 agencies defined them only partially. For example, one agency defined roles and responsibilities for the system owner but not for other key security personnel such as the chief information security officer and information system security officer. As a result, agency officials may not clearly understand their expected responsibilities and consequently, may not be able to carry out their duties correctly and effectively.

## Policies Lacked Adequate Instructions for Selecting Minimum Controls Evaluated during Periodic Testing

Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization.[9] NIST Special Publication 800-53 provides guidance to agencies for selecting these security controls, which serve as a starting point in determining and designing methods for testing the security controls. NIST specifies that agency security personnel must develop, document, and implement policies for consistent identification, testing, and evaluation of baseline controls.

Policies for selecting the minimum security controls evaluated during periodic tests for 11 of the 23 agencies were not always adequate. To illustrate, 7 of the 11 agencies reported having no specific policies or procedures for selecting the minimum baseline security controls, and the other 4 agencies' policies partially addressed the selection of these controls. For example, one agency's policy referenced NIST guidance for identifying controls, but it did not first specify the use of the NIST

[9]NIST, *Standards of Security Categorization of Federal Information and Information Systems*, (Federal Information Processing Standard (FIPS) Publication 199) establishes three levels of potential impact—high (severe or catastrophic), moderate (serious), and low (limited)—on organizational operations, assets, or individuals if a breach of security should occur. The standards are used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability.

standard when determining the system's impact level. In another example, an agency referenced NIST 800-53 guidance for selecting baseline controls, but it provided a checklist of controls to be tested that did not include the baseline controls as identified in NIST guidance. Without adequate instruction, security personnel may not consistently identify, test, and evaluate the baseline controls used to secure their systems.

## Policies Did Not Specify How to Identify and Test Common Controls

Identifying common security controls can increase efficiency in agencies' periodic testing. NIST 800-37 guidance defines a common security control as one that can be applied to one or more of an agency's information systems.[10] This guidance suggests that many of the management and operational controls—contingency planning, incident response, security training and awareness, personnel security, and physical security—needed to protect an information system may be excellent candidates for common security control status.[11] By identifying common controls, agencies can achieve efficiencies by testing common controls and using the results for multiple systems. For example, NIST states that an organizationwide approach to reusing and sharing test results can greatly enhance efficiencies and significantly reduce security program costs.

Policies for 22 of the 23 agencies we reviewed did not specify how to identify and test common security controls. For example, the security policies for 15 of the 22 agencies did not address the identification and testing of common security controls and policies and the other 7 agencies only partially addressed them. Specifically, the 7 agencies identified and tested some elements of common controls, but their policies did not describe how to identify, test, or share testing results with others. For example, one agency encouraged the use of common controls, but it did not specify how common controls were to be identified, how to test them, or how test results should be shared with others. In addition, another agency made reference to common controls as part of a pilot program, but no other discussion or reference was made regarding identifying and testing common security controls. Without policies and procedures that address or provide guidance for identifying and testing common controls, agencies may needlessly test common controls multiple times, thereby reducing efficiency and increasing costs for their periodic testing.

[10]NIST, *Guide for the Security Certification and Accreditation of Federal Information Systems*, SP 800-37 (Washington, D.C.: May 2004) p. 52.

[11]SP 800-37, p. 19.

## Policies Lacked Adequate Instructions for Determining the Depth and Breadth of Testing

An important element of efficient and effective testing is the consideration of the depth and breadth of agency testing. FISMA requires testing of the management, operational, and technical controls for every system at least annually. Moreover, Special Publication 800-37 states that it is not feasible or cost effective to monitor all of the security controls in an information system on a continuous basis and that the information system owner should select an appropriate subset of those controls for periodic assessment. In addition, OMB Memoranda M-05-15 and M-06-20 have identified three criteria for agency officials to consider when determining the depth and breadth of a review:

- The potential risk and magnitude of harm to the system or data.
- The relative comprehensiveness of the past year's review.
- The adequacy and successful implementation of a remediation plan to address weaknesses in the information system.

None of the 23 agencies' policies provided adequate instruction for determining the depth and breadth of periodic tests. Moreover, agencies did not incorporate the three OMB criteria into their policies as consideration for determining the depth and breadth of periodic testing. Security personnel reported that they do not fully understand how to apply the current guidance on determining the depth and breadth of controls testing and need further clarification. Until additional guidance clarifies how to determine the depth and breadth of testing, increased risk exists that agencies may not sufficiently test security controls in a cost-effective manner.

## Policies Did Not Always Describe a Process for Documenting Weaknesses in Remediation Plans

FISMA directs agencies to establish a process for remediating identified weaknesses in their information security policies and procedures. Key to an effective remediation plan is the accurate and complete inclusion of weaknesses identified during periodic testing. Remediation plans, also referred to as plans of action and milestones, should list all identified weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions. NIST 800-37 states that remediation plans need to be updated to address weaknesses identified as a result of periodic testing.

Policies for 10 of the 23 agencies did not fully describe a process for documenting identified control weaknesses. For example, 7 of the 10 agencies did not have policies that described a process for incorporating weaknesses identified during periodic security testing into remediation

plans. The remaining 3 agencies had policies on remediation plans, but these were in draft form only and provided no further description of the process for addressing weaknesses. Without adequate guidance for ensuring that identified weaknesses are incorporated into remediation plans, there is increased risk that weaknesses identified through security controls testing are not being properly addressed. Thus, agencies may not realize the full benefits of such testing and have limited assurance that the controls for their systems are functioning effectively.

## Six Case Study Agencies Did Not Effectively Implement Policies

None of the six case study agencies fully implemented their policies for periodic information security testing. During our review of 30 systems, we found implementation weaknesses at all six agencies. These weaknesses consisted of insufficient testing documentation, inadequately defined assessment methods, inadequate security testing, and lack of remedial actions included in testing plans, as shown in table 3.

**Table 3: Weaknesses in Six Agencies' Information Security Testing Methods**

| Agency systems | Insufficient testing documentation | Inadequately defined assessment method | Inadequate test of security control | Inadequately documented remedial actions in test plans |
|---|---|---|---|---|
| System 1 | X | X | X | X |
| System 2 | X | | X | X |
| System 3 | X | | X | X |
| System 4 | X | | X | X |
| System 5 | X | X | X | |
| System 6 | X | | | |
| System 7 | X | | X | |
| System 8 | X | | | |
| System 9[a] | X | X | X | X |
| System 10[a] | X | X | X | X |
| System 11 | X | | X | |
| System 12 | X | X | X | |
| System 13 | X | | X | |
| System 14 | X | | X | |
| System 15 | X | X | X | |
| System 16 | X | | X | X |
| System 17 | X | | X | X |
| System 18[a] | X | X | X | X |
| System 19 | X | | | X |

| Agency systems | Insufficient testing documentation | Inadequately defined assessment method | Inadequate test of security control | Inadequately documented remedial actions in test plans |
|---|---|---|---|---|
| System 20 | X | | X | X |
| System 21 | | | | |
| System 22 | X | | X | |
| System 23 | | | X | X |
| System 24 | X | | X | |
| System 25 | X | | X | X |
| System 26 | X | | X | X |
| System 27 | X | | | X |
| System 28 | X | | X | X |
| System 29 | X | | | X |
| System 30 | X | | X | X |
| **Total systems with weaknesses** | **28** | **7** | **24** | **18** |

Source: GAO analysis of agency FY 2005 test results (management, operational, and technical controls) and test documentation.

Note: "X" indicates weaknesses in testing implementation.

[a]The agency did not provide documentation for FY 2005 testing results for the system and, therefore, was given failing marks for all testing method categories.

## Agencies Did Not Have Sufficient Documentation on Testing

Testing documentation and supporting material serves as the basis for verifying that the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Test documents may include risk assessments, testing plans, the controls being tested, the results of the testing (security weaknesses and vulnerabilities), including results from previous security assessments, security reviews, or audits. Support materials may include procedures, reports, logs, and records showing evidence of security controls implementation.

Agencies did not sufficiently document periodic testing activities and results for 28 of the 30 systems reviewed. These examples ranged from no documentation to documentation that omitted key elements, such as risk assessments, testing plans, and test results. For example, testing plans did not provide enough detail to determine which tests were to be conducted or the scope of test coverage. In addition, one security manager reported that maintaining supporting documentation was not a common practice and that no supporting documentation or test records had been maintained until recently. Unless agencies develop and maintain sufficient

testing documentation, they will have limited evidence for making judgments about the security of their systems.

## Agencies Did Not Always Define Assessment Methods

NIST 800-37 identifies a variety of assessment methods such as interviewing, inspecting, studying, testing, demonstrating, and analyzing that agencies can use when evaluating their security controls. NIST guidelines describe these methods as interview, examine, and test.

- The **interview** method of assessment is the process of conducting focused discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence.

- The **examine** method of assessment is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (specifications, mechanisms, or activities). Similar to the interview method, the primary purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence.

- The **test** method of assessment is the process of exercising one or more assessment objects (limited to mechanisms or activities) under specified conditions to compare actual with expected behavior. NIST states that the results of assessments using these methods are to support the determination of overall security controls effectiveness.

Agencies did not fully define the assessment methods used to evaluate their system controls for 7 of the 30 systems reviewed. We found that the test plans, procedures, and testing results for 4 of the 7 systems did not identify how agencies evaluated system controls or whether they used interviews, examinations, or tests to determine the effectiveness of those controls. For the 3 remaining systems, agencies did not provide documentation to show what assessment methods were used. If agencies do not define assessment methods, they may not have information describing how that control was assessed. Without that information, agencies have limited assurance that those controls are being effectively tested or implemented.

## Agencies Did Not Always Adequately Test Security Controls

Once employed within an information system, security controls should be tested to determine the extent to which the controls are correctly implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. NIST states that assessments should be based on an examination of relevant documentation and a rigorous examination and testing of the controls. The

results of security testing contribute to the knowledge base of organization officials with regard to the security status of the information system and the overall risk to the operations and assets of the organization incurred by the operation of the system.

Agencies did not adequately test security controls for 24 of the 30 systems reviewed. The testing documentation showed no evidence of how testers assessed the security controls, whether they had tested the control as planned, or if they had conducted the test in accordance with the plan. In one example, testers reviewed management control policies; however, the testing guidelines required that the control be tested to determine if it had been effectively implemented. Unless agencies adequately test controls and document the results, they may not be able to measure the security status of their information systems, thereby limiting their ability to know whether controls are protecting their operations and assets.

### Agencies Did Not Include Remedial Actions in Testing Plans

FISMA requires that agencies document remedial actions that address deficiencies in the information security policies, procedures, and practices. NIST 800-37 states that the plan of action and milestones should describe the measures that have been implemented or planned to correct any deficiencies or weaknesses noted during the assessment of the security controls. NIST also states that remedial actions should be evaluated to determine if they effectively mitigate previously identified weaknesses or vulnerabilities in the information system.

For 18 of the 30 systems, agencies did not consistently test or evaluate the effectiveness of remedial actions for weaknesses identified through security control assessments. For example, testing documentation for some systems did not address the remedial actions that agencies had identified from prior assessments in their test plans. Unless agencies document and include remedial actions for previously identified control weaknesses in testing plans, agencies will have limited assurance that weaknesses have been corrected.

## Conclusions

Agencies have not adequately designed and effectively implemented policies for periodically testing information security controls. While almost all agencies had documented policies for security testing, the policies did not always adequately address elements important for effective testing. Ensuring that agencies' policies' are sufficient to address federal standards and guidelines helps to ensure their effective implementation in meeting FISMA requirements. While NIST has issued guidance on how agencies should apply the depth and breadth method for

testing security controls, agencies have not been documenting or implementing this approach in their testing. Also, agency officials reported that they did not understand this method.

Our review of 30 systems at six major federal agencies found weaknesses in testing practices and methods: documentation, testing methods, controls testing, and remedial actions in testing plans. Conducting effective periodic testing and evaluations of information security controls is a serious, pervasive, and crosscutting challenge to federal agencies, warranting increased attention from OMB. If these challenges are not addressed, federal agencies' information and operations may be at increased risk.

## Recommendations for Executive Action

Because of the governmentwide weaknesses in the design and implementation of agencies' policies for periodically testing and evaluating security controls, we recommend that the Director of the Office of Management and Budget take the following two actions:

- Instruct federal agencies to develop and implement policies on periodic testing and evaluation.
- Revise instructions for future FISMA reporting by requesting Inspectors General to report on the quality of agencies' periodic testing processes.

We also recommend that the Secretary of Commerce direct the Director, National Institute of Standards and Technology, to strengthen guidance on determining the depth and breadth of testing security controls.

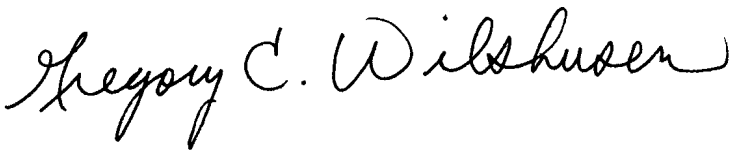
## Agency Comments

We received oral comments on a draft of this report from representatives of the Office of Management and Budget's Offices of Information and Regulatory Affairs and General Counsel. The representatives agreed to consider our recommendations as part of their oversight responsibilities for information security at federal agencies. The Deputy Secretary of the Department of Commerce provided written comments in response to our draft report (see app. II). He stated that the department agreed with our characterization of the National Institute of Standards and Technology's FISMA responsibilities and activities and also said that NIST is currently reviewing its guidance, including that for the depth and breadth of testing security controls.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies of the report to other interested congressional committees; the Director, Office of Management and Budget; and the Deputy Secretary of the Department of Commerce. We will make copies available to others on request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions about this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are acknowledged in appendix V.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

# Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine the extent to which federal agencies have adequately designed and effectively implemented policies for periodically testing and evaluating security controls. The scope of our review included (1) the 24 federal agencies,[1] focusing on reviewing their policies and procedures and responses to our survey and (2) a selection of 30 systems at 6 of these agencies, focusing on in-depth evaluations of their periodic controls testing and evaluation practices and methods.

To determine the adequacy and effectiveness of federal agencies' policies and procedures for testing and evaluating security controls for their information systems, we conducted a survey of the 24 major agencies, which included 21 questions for the agencies and 4 questions for the agencies' Inspectors General. We also reviewed the agencies' policies that were submitted in response to the surveys and compared them against six policy elements from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) standards and guidelines that we considered to be important for performing effective testing. The survey instruments were pretested with two federal information technology organizations—the Department of Defense and GAO's Office of the Chief Information Officer.

To assess the implementation of Federal Information Security Management Act of 2002 (FISMA) requirements, we reviewed 30 systems at the six case study agencies to determine whether policies for testing and evaluating security controls were effectively implemented. We selected for review the six agencies that reported the largest number of systems in their inventories of major systems, excluding agencies that had been recently reviewed by GAO.

We relied on FISMA standards and guidelines from OMB and NIST as criteria for evaluating agency testing and evaluation methods, policies, and procedures. These criteria were used to evaluate agency system documentation on the results of security controls testing, such as system security plans, testing results, testing plans and schedules, remedial action

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

plans, memoranda, and other artifacts used for information security testing. We collected fiscal year 2005 self assessment and testing artifacts and fiscal years 2004 and 2005 remediation plans in order to standardize the data for analysis. To augment our work, we considered the responses to our survey by the agencies and the Inspectors General.

We selected and examined 5 systems comprised of low, medium, and high impact general support systems and major applications for a total of 30 systems across the six agencies. Because we were evaluating the extent to which agencies periodically test and evaluate the effectiveness of security controls, we avoided selecting systems that had recently undergone certification and accreditation where more rigorous (independent) testing is conducted. In cases where an agency had recently certified and accredited the majority of its systems, we selected those having the oldest accreditation date within the selected time period. We evaluated government-owned and operated systems, and government-owned, contractor-operated systems; all were operational and none were under development. We did not select systems that were recently or currently under review by an Inspector General or those classified as national security or financial.

We performed our work in the Washington, D.C., metropolitan area and in three agency field offices in Pennsylvania, Texas, and Georgia, from November 2005 to July 2006, in accordance with generally accepted government auditing standards.

# Appendix II: Comments from the Department of Commerce

**THE DEPUTY SECRETARY OF COMMERCE**
Washington, D.C. 20230

September 25, 2006

Mr. Greg Wilshusen
Director
Information Security Issues
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the Government Accountability Office's draft report entitled "Agencies Need to Develop and Implement Adequate Policies for Periodic Testing" (GAO-06-960).

The Department of Commerce takes very seriously its role in implementing the Federal Information Security Management Act (FISMA). FISMA recognizes the importance of information security and the need for clear guidelines and steadfast, thorough implementation of those guidelines. The GAO report's references to the National Institute of Standards and Technology and the Institute's responsibilities and activities to assist agencies in implementing FISMA are accurate. We appreciate the GAO's identification of potential weaknesses in the processes federal agencies are using to implement FISMA. In fact, NIST already has identified this concern and is reviewing its guidance, including the depth and breadth of testing security controls, to assist agencies in strengthening their programs. I applaud your efforts to strengthen the security of federal information systems, and I look forward to receiving your final report.

Sincerely,

David A. Sampson

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Gregory C. Wilshusen, (202) 512-6244
Director, Information Security Issues

## Staff Acknowledgments

In addition to the individual named above, Suzanne Lightman (Assistant Director), Ayannah Buford, Larry Crosland, Neil Doherty, Nicole Garofalo, Nancy Glover, Joel Grossman, David Hong, John Ortiz, Jerome Sandau, Donald Sebers, Jenniffer Wilson, and Charles Youman made key contributions to this report.

## 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