United States General Accounting Office

GAO

Report to Congressional Requesters

June 2004

INFORMATION SECURITY

Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation

GAO-04-376

June 2004

INFORMATION SECURITY

Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-376, a report to the Chairman, House Committee on Government Reform and the Chairman of its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Why GAO Did This Study

The Office of Management and Budget (OMB) requires agencies to certify the security controls of their information systems and to formally authorize and accept the risk associated with their operation (a process known as accreditation). These processes support requirements of the Federal Information Security Management Act of 2002 (FISMA). Further, OMB requires agencies to report the number of systems authorized following certification and accreditation as one of the key FISMA performance measures.

In response to the committee and subcommittee request, GAO (1) identified existing governmentwide requirements and guidelines for certifying and accrediting information systems, (2) determined the extent to which agencies have reported their systems as certified and accredited, and (3) assessed whether their processes provide consistent, comparable results and adequate information for authorizing officials.

What GAO Recommends

GAO is making recommendations to the Director, Office of Management and Budget, to help ensure that agencies' certification and accreditation processes consistently provide adequate and effective information security controls. In oral comments on a draft of this report, OMB officials generally agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-376.

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

What GAO Found

The National Institute of Standards and Technology (NIST) and other agencies, including the Department of Defense, have provided guidance for the certification and accreditation of federal information systems. This guidance includes new guidelines just issued by NIST, which emphasize a model of continuous monitoring, as well as compliance with FISMA-required standards for minimum-security controls. Many agencies report that they have begun to use the new guidance in their certification and accreditation processes.

The reported percentage of systems certified and accredited for operation as of the first half of 2004 was 63 percent for 24 major federal agencies. However, the picture is not uniform across the government, with 7 of the agencies reporting greater than 90 percent of their systems certified and accredited but 6 reporting fewer than half. GAO's analyses also highlighted instances in which agencies do not consistently report FISMA performance measurement data, as well as other factors that lessen the usefulness of these data, such as the limited assurance of data reliability and quality.

All the agencies GAO surveyed reported that their certification and accreditation processes met criteria consistent with those identified in federal guidance, such as a current risk assessment and security control evaluation. However, our review of documentation for the certification and accreditation of 32 selected systems at four of these agencies showed that these criteria were not always met (see chart)—results similar to those found by agency inspectors general. Further, three of these four agencies did not have routine quality review processes to determine whether such criteria are met—processes that could help agency accrediting officials receive consistent information on which to base their decisions. Several agencies cited obstacles in implementing their certification and accreditation processes, including resource and staffing limitations. Some agencies have taken actions to improve their processes, such as redefining system boundaries to better manage systems.

Number and Percentage of 32 Selected Agency Systems Meeting Specific Certification and Accreditation Criteria

Criterion	Number of systems meeting criterion (percentage)	
Current risk assessment?	23	(72%)
Current security plan?	26	(81%)
Controls tested?	22	(69%)
Contingency plan?	19	(59%)
Contingency plan tested?	8	(42%)[a]
Plan with milestones prepared for weaknesses?	17	(81%)[b]
Residual risk identified?	17	(53%)

Source: GAO based on agency data.

[a]Percentage based on the total of 19 systems with contingency plans.

[b]Percentage based on 21 systems where plans were required to correct identified weaknesses.

Contents

Abbreviations

CIO	chief information officer
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IG	inspector general
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

June 28, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Office of Management and Budget (OMB) information security policy requires agency management officials to formally authorize each of their information systems to process, store, or transmit information, and to accept the risk associated with their operation. This authorization *(accreditation)* decision 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. As required by OMB, agencies are also 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).

The Federal Information Security Management Act of 2002 (FISMA) provides the overall framework for ensuring the effectiveness of information security controls that support federal operations and assets and requires agencies and OMB to report annually to the Congress on their information security programs.[1] As part of its responsibilities under FISMA, OMB requires agencies to report the number of systems authorized for processing following certification and accreditation as one of the key performance measures for their information security programs. Although not required by FISMA, OMB considers certification and accreditation to be an important information security quality control, and this process reinforces several of the act's requirements, including those for a system risk assessment, a security plan, control testing, and contingency planning. Further, OMB emphasized the significance of this process in its *FY 2003 Report to Congress on Federal Government Information Security*

[1]Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, P.L. 107-347, December 17, 2002.

Management,[2] in which it noted that most security weaknesses could be found in operational systems that either have never been certified or accredited, or whose certification and accreditation is out of date.

OMB's information technology policies and its authorities under FISMA generally do not apply to national security systems.[3] However, the head of each agency operating or exercising control of a national security system is responsible for complying with FISMA requirements, and agencies such as the Department of Defense (DOD) have established policies requiring certification and accreditation of national security systems.

Objectives, Scope, and Methodology

In response to your request, our objectives were to

- identify existing governmentwide requirements and guidelines for certifying and accrediting federal information systems,
- determine the extent to which federal agencies have reported that their information systems are certified and accredited, and
- assess whether agencies' certification and accreditation processes provide (1) consistent and comparable results, and (2) adequate information for authorizing officials to understand risks and make informed decisions.

To determine what requirements and guidelines exist for agencies to follow in certifying and accrediting their systems, we obtained and reviewed information security policies and guidance issued by OMB, the National Institute of Standards and Technology (NIST), and DOD, including its

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

[3]As currently defined in FISMA, the term "national security system" 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.

National Security Agency and the Committee on National Security Systems, which is chaired by DOD's Chief Information Officer. We also met with representatives from these agencies to discuss these policies and guidance, as well as to identify any planned revisions or additional guidance. This included guidance for both non-national security and national security systems. In addition, to help address all three of our objectives, we conducted a survey of 24 major departments and agencies, which included questions on the guidance they follow in certifying and accrediting their systems.[4]

To determine the extent to which agencies have certified and accredited their systems, we analyzed performance measurement data reported to OMB by the agencies for their fiscal year 2002 and 2003 annual reporting and for their March 2004 quarterly updates, which was due to OMB on March 15, 2004. This performance measurement data largely reflects non-national security systems, but some agencies also included data on national security systems.

To assess whether agencies' certification and accreditation processes provide consistent and comparable results and adequate information for authorizing officials, we analyzed the results of our survey to determine the extent to which agencies reported that their processes addressed specific criteria identified in federal certification and accreditation guidance, such as a current risk assessment and evidence of control testing. In addition, for selected systems at four agencies—the Departments of Commerce and Energy, the Environmental Protection Agency (EPA), and the National Aeronautics and Space Administration (NASA)—we also analyzed certification and accreditation documentation to determine whether the certification and accreditation criteria were met. We selected these agencies based primarily on the high percentages of certified and accredited systems they reported to OMB in their annual reports for fiscal years 2002 and 2003.

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

We did not validate the accuracy of the data in agencies' FISMA reports, survey responses, or system certification and accreditation documentation. However, we considered the data within the context of a significant body of existing knowledge and evidence about agency certification and accreditation practices and, to the extent that they addressed their agencies' certification and accreditation efforts, reviewed and compared the results of agencies' inspectors general (IG) fiscal year 2003 FISMA independent evaluations.

We performed our work in the Washington, D.C., metropolitan area from September 2003 to June 2004, in accordance with generally accepted government auditing standards.

Results in Brief

With NIST's recent issuance of new guidelines, certification and accreditation processes for federal information systems continue to evolve. To be used for non-national security systems, the new guidelines update previous NIST guidance to reflect today's more distributed computing environment in which systems are constantly evolving and require real-time, on-going monitoring. These guidelines also incorporate other recent NIST standards and guidance required by FISMA, including those to categorize and provide recommended security controls for federal information systems. Other agencies have also developed certification and accreditation guidance, particularly for national security systems.

For the 24 agencies we surveyed, the average percentage of systems authorized after certification and accreditation was 63 percent for the first half of fiscal year 2004. However, the status of individual agencies was mixed, with 7 agencies reporting certification and accreditation for 90 percent or more of their systems, but 6 reporting that fewer than half of their systems were certified and accredited. Our analysis also highlighted inconsistencies in the way agencies report such certification and accreditation performance data. For example, national security systems are included in some reported agency totals, but not in others. Further, there are other factors that lessen the usefulness of these and other FISMA performance data, including the limited assurance of data reliability and quality and the need to refine reporting requirements to provide better information on the status of agencies' information security efforts.

All the agencies we surveyed reported that their certification and accreditation processes met criteria consistent with those identified in federal guidance, such as a current risk assessment, security control

evaluation, and an accreditation statement that indicates the level of residual risk being accepted by the authorizing official. However, our review of certification and accreditation documentation for selected systems at four agencies showed that these criteria were not always met—results similar to those found by inspectors general (IGs) in their FISMA evaluations. Further, three of these four agencies did not have processes to routinely review the quality of their certification and accreditation efforts—processes that could help agencies ensure that accrediting officials consistently receive sufficient information on which to base their decisions.

Survey results also identified potential challenges and obstacles to agencies' certification and accreditation processes, particularly regarding funding and staffing issues. The new NIST guidelines suggest ways to help address resource issues, such as reusing and sharing of security control development, implementation, and assessment-related information. Some agencies had also undertaken successful practices in implementing their certification and accreditation processes that can help address such challenges, such as redefining system boundaries to better organize their efforts and manage systems.

This report contains recommendations to the Director of OMB, including that OMB's information security policy and guidance encourage agencies to ensure that periodic testing and evaluation of information security controls, as required by FISMA, include assessing the quality of security certifications and accreditations to ensure that decisions are based on consistent consideration of key criteria outlined in federal guidance. We also recommend that OMB consider changes to its FISMA reporting guidance, including requiring reporting on the quality and consistency of certifications and accreditations and encouraging the IGs to assess agency processes and test agency-reported performance data as part of their FISMA-mandated independent evaluations.

In oral comments on a draft of this report, OMB representatives in its Office of Information and Regulatory Affairs and Office of General Counsel agreed that the quality of agency certification and accreditation processes varies, and generally agreed with our recommendations. In addition to the recent issuance of certification and accreditation guidance by NIST, OMB believes that existing guidance, including its Circular A-130 and FISMA implementing guidance, is adequate to ensure that implementation of certification and accreditation is effective. Further, OMB stated that its planned fiscal year 2004 FISMA guidance to the agencies would address

many of the issues in our report. The Department of Commerce provided written comments on a draft of this report (see app. I), and we also received written and oral technical comments from the Departments of Defense and Energy, EPA, NASA, and NIST. Comments from all these agencies have been incorporated into the report, as appropriate.

Background

FISMA permanently authorized information security program, evaluation, and reporting requirements for federal agencies. As a key element of agencies' implementation of FISMA requirements, OMB has continued to emphasize its longstanding policy of requiring a management official to formally authorize an information system to process information and accept the risk associated with its operation based on a formal evaluation of the system's security controls. Further, compliance with new FISMA-required standards and guidance will become important considerations in the certification and accreditation of agency systems.

FISMA Establishes Federal Information Security Requirements

Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA assigns specific information security responsibilities to OMB, NIST, agency heads, chief information officers (CIO), and IGs. For OMB, these responsibilities include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security; and reviewing at least annually, and approving or disapproving, agency information security programs. FISMA continues to delegate OMB responsibilities for national security systems to the Secretary of Defense and the Director of Central Intelligence. Therefore, OMB's information technology policies and its authorities under FISMA, as well as federal information system standards and guidelines developed by NIST, generally do not apply to national security systems. However, according to FISMA, the head of each agency operating or exercising control of a national security system is responsible for providing information security protections commensurate with the risk and magnitude of harm, implementing information security policies and practices as required by standards and guidelines for national security systems, and complying with FISMA requirements.

FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency,

including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- 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.

In addition to these information security program requirements, FISMA also requires each agency to develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or 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.

Under FISMA, each agency must 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.

Other major FISMA provisions require NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. In conjunction with DOD and the National Security Agency, NIST is responsible for developing guidelines for identifying an information system as a national security system.

OMB Continues to Emphasize Certification and Accreditation

Since the mid-1980s, OMB policy for information technology (IT) management has required that an agency official attest to the adequacy of an information system's security safeguards. As currently described in its Circular A-130,[5] OMB requires federal agencies to ensure that a management official authorizes in writing the use of each general support system or major application based on implementation of its security plan before beginning or significantly changing its processing.[6] This management approval, or accreditation, is the authorization of an IT

[5]Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130, Transmittal Memorandum No. 4, Appendix III, *Security of Federal Automated Information Resources*, November 28, 2000.

[6]Per OMB Circular No. A-130, a *general support system* is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. An *application* means the use of information resources to satisfy a specific set of user requirements, and a *major application* is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

system to process, store, or transmit information that provides a form of quality control and challenges managers and technical staff to find the best fit for security given technical constraints, operational constraints, and mission requirements. The accreditation decision is based on the implementation of an agreed-upon set of management, operational, and technical controls for a system, and is supported by a comprehensive evaluation or certification of these security controls that provides the necessary information for a management official to formally declare that a system is approved to operate at an acceptable level of risk. OMB policy also specifies the following:

- Security staff should not make the accreditation decision. In general, the security official is closer to the day-to-day operation of the system and will direct or perform security tasks, while the authorizing official will normally have general responsibility for the organization supported by the system.

- 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).

With the implementation of FISMA, OMB has continued to emphasize system certification and accreditation by requiring agencies to report the number of systems certified and accredited as one of the key performance measures for reporting under these laws. Continuing this requirement as part of its overall authority under FISMA to develop and oversee the implementation of policies, principles, standards, and guidelines on information security, OMB has taken other steps to help integrate certification and accreditation into agencies' information security programs. For example, in the President's fiscal year 2004 budget, OMB established a governmentwide goal that 80 percent of federal IT systems be certified and accredited by the end of calendar year 2003. According to OMB, it also monitors the certification and accreditation of major systems through the budget process with the possibility that funding could be denied for those IT investments that do not meet security requirements, such as not being fully certified and accredited prior to becoming operational. In addition, in its fiscal year 2003 report to the Congress, OMB outlined a plan of action to improve performance in IT security that identifies specific steps it will pursue to assist agencies. One such step concerns the *President's Management Agenda Scorecard*, where one criterion that agencies must meet to "get to green" under the Expanding

E-Government Scorecard for IT security is to attain certification and accreditation for 90 percent of their operational IT systems.

FISMA-Required Standards and Guidance Are Important Considerations

NIST has issued a number of information security standards and guidance documents that contribute to the certification and accreditation process, such as its guidance on conducting risk assessments and on the format and content of security plans.[7] In addition, as part of its statutory responsibilities under FISMA, NIST has issued additional standards and guidance that will be important considerations in agencies' future certification and accreditation efforts. As we reported in our March 2004 testimony,[8] these included the following:

- In December 2003 NIST issued the final version of its *Standards for Security Categorization of Federal Information and Information Systems* (FIPS Publication 199). NIST was required to submit these categorization standards to the Secretary of Commerce for promulgation no later than 12 months after FISMA was enacted. These standards are intended to provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs, and consistent reporting to OMB and the Congress on the adequacy and effectiveness of information security policies, procedures, and practices. To help establish security categories for both information and information systems, the standards establish three levels of potential impact on organizational operations, assets, or individuals should a breach of security occur—**high** (severe or catastrophic), **moderate** (serious), and **low** (limited)—and are used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability.[9] Once determined, security categories are to

[7]National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30 (July 2002); and *Guide for Developing Security Plans for Information Technology Systems* Special Publication 800-18 (December 1998).

[8]U.S. General Accounting Office, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, GAO-04-483T (Washington, D.C.: March 16, 2004).

[9]The loss of confidentiality is the unauthorized disclosure of information, the loss of integrity is the unauthorized modification or destruction of information, and the loss of availability is the disruption of access to or use of information or an information system.

be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

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

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

Certification and Accreditation Guidance Is Provided by NIST and Other Responsible Agencies

For more than 20 years, NIST guidance has provided a basic framework for federal agencies to establish a certification and accreditation process. As part of its efforts to support FISMA, NIST has recently issued new certification and accreditation guidance intended, in part, to create more complete, reliable, and trustworthy information for accreditation decisions. In addition, other agencies responsible for national security systems, such as DOD, have also developed certification and accredition guidance.

Early NIST Guidance Provides Basic Framework

In September 1983, the National Bureau of Standards, the predecessor to NIST, issued Federal Information Processing Standards (FIPS) Publication 102, *Guideline for Computer Security Certification and Accreditation*. Identified by OMB in its Circular A-130, this guidance provided federal agencies with a basic framework for establishing a certification and accreditation process intended to help improve management control over computer security and increase computer security awareness throughout the organization.

FIPS Publication 102 focused on establishing a certification and accreditation process for sensitive applications, that is, those applications that require a measure of protection because they process sensitive information or because of the risk or magnitude of loss or harm that could result from the improper operation or deliberate manipulation of them.[10] For less sensitive applications, the guidance advised that a less elaborate process could be used. Elements of the certification and accreditation process described by this guidance include the following:

- *Roles and responsibilities*. Several roles and responsibilities were identified for the certification and accreditation process, including the following key roles:
  - *Accrediting officials* are the agency officials who have authority to accept an application's security safeguards and issue an accreditation statement that records the decision. These officials must possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies. An accrediting official or group of officials may be responsible for several applications, but there is typically only one official or group assigned to each application. In general, the more sensitive the application, the higher the accrediting officials are in the organization.
  - The *application certification manager* is responsible for managing a specific certification effort, including planning the effort and overseeing the production of the security evaluation report. To help

[10]FIPS Publication 102 defined a computer application as the use(s) for which a computer system is intentionally employed. Further, an application broadly represents a variety of certification entities, including software programs, hardware components, applications, systems, terminals, networks, installations, and other entities.

ensure an objective evaluation, this person is to be as independent as possible from the application being certified.

- *Security evaluators* are reponsible for performing the technical security evaluation tasks and providing expert technical judgements in their areas of specialization. The required specializations vary with each application, and the more detailed the evaluation, the greater the specialization required. Useful specialties identified included application analysts, system analysts, engineers, application programmers, and system programmers. Security evaluators are to be as independent as possible from the application.

- *Evaluation techniques for security certification.* This element describes the various computer security evaluations that can use security requirements as criteria and, thus, can be used for certification. Specifically, these include (1) an analysis of risk to understand the security problem; (2) validation, verification, and testing performed in developing the application and throughout its lifecycle; (3) a security safeguard evaluation performed by people independent of the application, but internal to the organizational division in which the application resides (which may include a security officer); and (4) an electronic data processing audit performed within internal audit to assess the controls in an organization's system that rely on computers.

- *Performing a certification.* The certification process described consists of five steps: (1) planning the effort to understand the issues for the entire system and to place boundaries on the work; (2) collecting critical data and information such as the risk analysis, inputs, processing steps, outputs, and a listing of application system controls; (3) performing a basic evaluation of security requirements and functions, control implementation, and the implementation method; (4) in the event that a basic evaluation does not provide enough evidence for certification, performing a detailed evaluation to analyze the quality of security safeguards; and (5) preparing a security evaluation report—the primary product of a certification—that includes both technical and management security recommendations and a proposed accreditation statement.

- *Security evaluation report.* The format and contents of the security evaluation report are described, including major findings, recommended corrective actions, and a proposed accreditation statement. In particular, the major findings are to include both proposed residual

vulnerabilities and proposed vulnerabilities requiring correction. Depending on the seriousness of the security flaw identified, implementation of an application under development may be delayed or an operational application may require removal from service. However, other intermediate alternatives were also identified, such as withholding accreditiation pending completion of corrections, adding procedural security controls, restricting the application to process only nonsensitive or minimally sensitive data, or removing especially vulnerable application functions or components.

- *The accreditation decision and statement.* The accrediting official essentially uses the security evaluation report to evaluate the certification evidence, decides on the acceptability of security safeguards, approves corrective actions, signs the accreditation statement, and ensures that corrective actions are accomplished. The accreditation statement officially documents the explicit acceptance of responsibility for computer security, and should identify any restrictions of operation for the application, as well as any corrective actions.

- *Recertification and reaccreditation.* The guidance explains that certification and accreditation are not permanent, and may need to be performed again for reasons including changes to the application, changes in requirements, passage of a time interval (such as the 3-year interval established by OMB), the occurrence of a significant violation, or audit or evaluation findings.

New NIST Guidance Intended to Improve the Process

In May 2004, NIST issued its *Guide for the Security Certification and Accreditation of Federal Information Systems* (Special Publication 800-37) to be used in certifying and accrediting non-national security systems.[11] Developed as part of NIST's project to promote the development of standards and guidelines to support FISMA, this new guide is to replace FIPS Publication 102 when it is rescinded (which, according to a NIST official, should take place in the next six months). At the time of our survey, all 24 agencies reported that they planned to adopt or modify their existing guidance to be consistent with Special Publication 800-37, and 14 agencies reported they already used a draft version of the guidance.

[11]National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Special Publication 800-37– Final (May 2004).

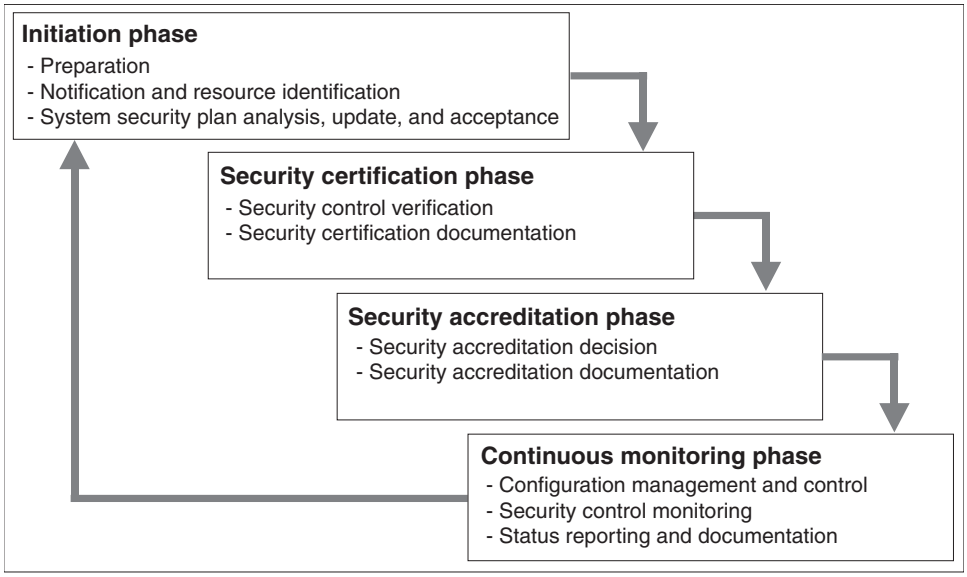
As discussed in the guide, its overall purpose is to help achieve more secure information systems within the federal government by

- enabling more consistent, comparable, and repeatable evaluations of security controls applied to federal information systems;
- promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and
- creating more complete, reliable, and trustworthy information for authorizing officials to facilitate more informed security accreditation decisions.

Further, NIST encourages state, local, and tribal governments, as well as private-sector organizations comprising the critical infrastructure of the United States, to consider the use of these guidelines, as appropriate.

The new NIST guidance updates the process described in FIPS Publication 102. For example, according to a NIST official, the certification process in FIPS Publication 102 was a static evaluation of systems where systems were tested at a given, single point in time to determine the overall risk. Further, this official stated that although this process was an adequate measure 20 years ago, in today's more distributed computing environment where systems are constantly evolving, real-time, ongoing monitoring is required. As a result, the new process described in Special Publication 800-37 identifies four phases, which includes a continuous monitoring phase. Each of these phases—initiation, security certification, security accreditation, and continuous monitoring—consists of a set of defined tasks and subtasks that are to be carried out by the various roles assigned for the process. To help illustrate this process, figure 1 provides a high-level view, along with the key tasks associated with each phase.

Figure 1: NIST Security Certification and Accreditation Process



Source: NIST Special Publication 800-37.

The new guidance continues to emphasize the assessment of risk and the development of system security plans as two important activities in an agency's information security program that directly support the security accreditation process. It also emphasizes the importance of the security assessment (certification) in the accreditation process to help ensure that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The guide also emphasizes several new concepts and includes other significant changes from FIPS Publication 102, such as the incorporation of FISMA-mandated standards and guidelines into the process. This and other new concepts and changes are discussed below.

FISMA-Required Standards Are Incorporated

FISMA-required standards issued by NIST are incorporated as an integral part of the new certification and accreditation process. The certification and accreditation guideline identifies specific examples of how these standards are considered, including the following:

- The security category of an information system (overall potential impact level of high, moderate, or low) assigned based on FIPS Publication 199 influences the initial selection of security controls from NIST Special Publication 800-53 and the initial selection of assessment methods and procedures from NIST Special Publication 800-53A. The level of effort applied to the certification and accreditation tasks and subtasks should be commensurate with the strength of the security controls selected and the rigor and formality of the assessment methods and procedures selected. Further, because of the limited adverse effect expected for low-impact systems, the scalability of the certification and accreditation process for these systems results in the elimination of the independent certification agent, the incorporation of self-assessment activities, and a reduction in the associated level of supporting documentation and paperwork.

- The security category of the information system should guide the degree of independence of the certification agent. When the potential impact on agency operations, agency assets, or individuals is low, a self-assessment activity may be reasonable and appropriate and not require an independent certification agent. When the potential agency-level impact is moderate or high, certification agent independence is needed and justified.

- Security categories can play an important part in helping to define the accreditation boundary for an information system by partitioning the agency's information systems according to the criticality or sensitivity of the systems and the importance of those systems in accomplishing the agency's mission.

- Information systems, especially mission-critical or high-impact systems, should not be operating with significant security vulnerabilities requiring extended remediation time.

Additional Roles and Responsibilities

The guide defines additional participants in the certification and accreditation process and provides further clarification of the responsibilities of others. For example, it identifies the roles played by the chief information officer, senior agency information security officer, information system owner, information system security officer, certification agent, and user representative(s). The guide also creates a new role of authorizing official's *designated representative* to act on the authorizing official's behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation

process. The designated representative interacts with other participants in the process; can be empowered by the authorizing official to make certain decisions, such as acceptance of the system security plan; and may also be called upon to prepare the final security accreditation package. However, the authority to make the security accreditation decision and to sign the associated decision letter remains with the authorizing official and cannot be delegated to the designated representative.

The guide continues to identify the authorizing official as the official who, through the accreditation decision, assumes responsibility and is accountable for the risks associated with operating an information system. It also indicates that this official should have the authority to oversee the budget or business operations of the information system within the agency and is often called upon to approve system security requirements and system security plans. Further, in addition to authorizing system operation, the authorizing official can issue an interim authorization to operate the system under specific terms and conditions or deny authorization to operate the system (or if the system is already operational, halt operations) if unacceptable security risks exist.

Common Security Controls

The NIST guideline describes common security controls that can apply to all agency information systems, a group of information systems at a specific site (sometimes associated with the terms site certification/accreditation), or common information systems, subsystems, or applications (that is, common hardware software, and/or firmware) deployed at multiple operational sites (sometimes associated with the terms type certification/accreditation). Common security controls are typically identified during a collaborative agencywide process with the involvement of the senior agency information security officer, authorizing officials, information system owners, and information system security officers. The results from the assessment of such controls can be used to support the security certification and accreditation processes of agency information systems where those controls have been applied. Further, many of the management and operational controls (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, and physical security controls) needed to protect an information system may be excellent candidates for common security control status.

Conditions for Interim Authorization to Operate

If, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, but there is an overarching mission necessity

to place the information system into operation or continue its operation, an *interim authorization to operate* may be issued. An interim authorization to operate is provided when the identified security vulnerabilities in the information system resulting from deficiencies in the planned or implemented security controls are significant, but can be addressed in a timely manner. Further, an interim authorization provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time. These terms and conditions are established by the authorizing official and convey limitations on information system operations.

Documentation of Security Accreditation

The accreditation package documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system. The package is generally compiled and submitted by the information system owner, who receives inputs from the information system security officer, certification agent, and senior agency information security officer. The package contains the approved system security plan, security assessment report, and plan of action and milestones,[12] and is submitted to the authorizing official or designated representative.

The accreditation decision letter is used to transmit the decision from the authorizing official to the information system owner. Prepared for the authorizing official by the designated representative, the final letter should contain the accreditation decision, supporting rationale for the decision, and terms and conditions for the authorization. It also indicates whether the system is fully authorized to operate, authorized to operate on an interim basis under strict terms and conditions, or not authorized to operate. The accreditation decision letter is attached to the original accreditation package and returned to the information system owner, who maintains this documentation.

[12]Used by OMB to monitor the status of remediation efforts for FISMA, plans of action and milestones are required for all programs and systems where an IT security weakness has been found. The plan lists the weaknesses and shows estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

Transition to New Certification and Accreditation Guidance

Although OMB representatives state that its Circular A-130 is being revised, the current version does not reflect FISMA requirements or recent guidance issued by NIST. Although OMB requires agencies to ensure that their policies, standards, and procedures are consistent with NIST guidance, specifically requiring security certification and accreditation processes consistent with NIST's Special Publication 800-37 guidance in OMB policy and guidance would help ensure consistency in implementing such processes. To help with the transition to NIST's Special Publication 800-37, in July 2003 OMB issued interim guidance summarizing the minimum activities that agencies should implement to comply with the certification and accreditation requirement in OMB Circular A-130, as well as to facilitate easy alignment when the NIST guideline is finalized. Among other things, the interim guidance encouraged the use of NIST's *Security Self-Assessment Guide for Information Technology Systems* for conducting certification reviews, which uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured.[13]

Responsible Agencies Provide Guidance for National Security Systems

Because OMB's authorities and NIST guidance are not applicable to national security systems, agencies responsible for these systems have also issued certification and accreditation guidance. The processes and criteria established by this guidance are similar to those required by NIST guidance for non-national security systems, that is, they require risk assessments, verification of security requirements in a security plan or other document, testing of security controls, and formal authorization by an authorizing official (or designated approving/accrediting authority, as referred to by some agencies). Guidance issued by other agencies include the following:

[13]National Institute of Standards and Technology, Security *Self-Assessment Guide for Information Technology Systems*, Special Publication 800-26 (November 2001).

- DOD Directive 8500.1 on information assurance requires the heads of all components to comply with established accreditation processes required for all DOD information systems, and DOD Instruction Number 5200.40 creates the *DOD Information Technology Security Certification and Accreditation Process (DITSCAP)* for both unclassified and classified automated information systems, networks, and sites in the department.[14] Organized within four phases—definition, verification, validation, and post accreditation—a key element of DITSCAP is the development of an agreement among the program manager, the designated approving authority, the certification authority, and the user representative during the definition phase. This agreement (the System Security Authorization Agreement) is used throughout the entire DITSCAP to guide actions, document decisions, specify security requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security.

- The *National Information Assurance Certification and Accreditation Process*, issued by the DOD-chaired National Security Telecommunications and Information Systems Security Committee (now the Committee on National Security Systems), establishes minimum national standards for certifying and accrediting national security systems.[15] A key element of this guidance is the agreement among the program manager, designated approving authority (accreditor), certification agent (certifier), and user representative, who resolve critical schedule, budget, security, functionality, and performance issues. Agreements are documented in a System Security Authorization Agreement, which is used to guide and document the results of the certification and accreditation.

[14]Department of Defense, Information Assurance (IA), Directive 8500.1 (Oct. 24, 2002); and *DOD Information Technology Security Certification and Accreditation Process (DITSCAP)*, Instruction Number 5200.40 (Dec. 30, 1997).

[15]National Security Telecommunications and Information Systems Security Committee, *National Information Assurance Certification and Accreditation Process (NIACAP)*, NSTISSI No. 1000 (April 2000).

- Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*, and its implementation manual provide policy and procedures for the security and protection of systems that create, process, store, and transmit intelligence information, as well as define and mandate the use of a risk management process and a certification and accreditation process.[16] The certification process described by this guidance includes validation that appropriate levels of concern for integrity and availability and an appropriate confidentiality protection level have been selected from tables and descriptions provided in the implementation manual, and that required safeguards have been implemented as described in the system security plan. This process also considers other factors associated with the information system and its operational environment, including mission criticality, functional requirements, information system security boundaries, threat and vulnerability assessments, and other intelligence-related factors.

Reported Percentages of Systems Certified and Accredited Vary Widely

For the 24 agencies we surveyed, the average percentage of systems authorized after certification and accreditation was 63 percent for the first half of fiscal year 2004. However, the status at individual agencies was mixed, with six reporting that they have certified and accredited less than half of their systems. Our analysis also highlighted inconsistencies in the way agencies report such certification and accreditation performance data. For example, national security systems are included in some reported agency totals, but not in others. Further, there are other factors that lessen the usefulness of these and other FISMA performance data, including the limited assurance of data reliability and quality and the need to refine reporting requirements to provide better information on the status of agencies' information security efforts.

Progress by Individual Agencies Is Mixed

The average percentage of systems authorized after certification and accreditation reported by the 24 agencies was 63 percent for the first half of fiscal year 2004. This compares to 48 percent for fiscal year 2002 and to 62 percent for fiscal year 2003. Despite this reported overall progress, the

[16]Director of Central Intelligence, Protecting Sensitive Compartmented Information Within Information Systems, Directive 6/3 (DCID 6/3) (June 5, 1999); and Protecting Sensitive Compartmented Information Within Information Systems (DCID 6/3)—Manual (Aug. 1, 2000).

status of individual agencies varies widely. For example, 7 agencies reported more than 90 percent of their systems were certified and accredited for the first half of fiscal year 2004, including the Nuclear Regulatory Commission, which reported 100 percent. In contrast, 6 agencies reported less than half of their systems were certified and accredited, including the Department of Housing and Urban Development, which reported none. Table 1 summarizes the percentages reported by the agencies for the 2 fiscal years and for the first half of fiscal year 2004.

Table 1: Agency Systems Reported as Authorized After Certification and Accreditation

	Percentage by fiscal year		
Department or agency	**2002**	**2003**	**1st Half 2004**
Agency for International Development	100	88	70
Agriculture	8	14	0[b]
Commerce	77	97	96
Defense	55	80	77
Education	0	13	61
Energy	46	83	86
Environmental Protection Agency	87	94	94
General Services Administration	13	22	58
Health and Human Services	11	41	59
Homeland Security	[a]	42	59
Housing and Urban Development	72	9	0[b]
Interior	22	10	19
Justice	76	79	88
Labor	70	58	85
National Aeronautics and Space Administration	89	98	98
National Science Foundation	30	95	95
Nuclear Regulatory Commission	50	90	100
Office of Personnel Management	0	91	94
Small Business Administration	65	74	87
Social Security Administration	100	100	100
State	0	36	38
Transportation	8	33	49
Treasury	43	24	58
Veterans Affairs	31	39	12
Average percentage	**48**	**62**	**63**

Sources: OMB, agencies (data), and GAO (analysis).

[a]The Department of Homeland Security began its FISMA reporting in fiscal year 2003. However, the fiscal year 2002 percentage included the Federal Emergency Management Agency, which became part of the new department. Components of other agencies also became part of the department, including the U.S. Coast Guard and U.S. Customs Service, which were formerly within the Departments of Transportation and the Treasury, respectively.

[b]Agriculture and Housing and Urban Development officials indicated that concerns over the quality and consistency of their certification and accreditation processes were the basis for reporting no certified and accredited systems during the first half of 2004. Both agencies have sought the services of contractors to assist them in establishing a certification and accreditation process and in ensuring that

most, if not all, of their agencies' systems are certified and accredited by the end of calendar year 2004.

As shown in table 1, in comparing fiscal year 2003 results with those shown for the first half of 2004, agencies showing the greatest increase included Education (+48 percentage points) and the General Services Administration (+ 36 percentage points). On the other hand, some showed decreasing percentages, including Veterans Affairs (-27 percentage points) and Agriculture (-14 percentage points).

In responding to our survey, agencies cited several reasons why not all of their systems were certified and accredited. These reasons included systems' being decommissioned or retired; agency efforts' being focused on the most critical systems, with the less critical systems' being scheduled later; higher priority operational requirements and limited funding; and legacy systems' being unable to support required technical controls.

Our analysis of survey responses also highlighted instances in which agencies report performance measurement data differently. For example, some agencies, such as Energy, include both non-national security and national security systems in their reported performance data, while others, such as NASA, do not include their national security systems. As another example, DOD includes systems with interim authorization to operate among those systems reported as certified and accredited because, according to DOD officials, interim authorizations still represent a management approval to operate. In contrast, the National Science Foundation does not report systems with interim authorization to operate as certified and accredited. OMB instructions for fiscal year 2003 FISMA reporting were not specific regarding whether national security systems should be reflected in agency performance measurement data nor did they address how to report systems with interim authorization to operate. OMB representatives indicated that national security systems are to be reflected in reporting performance measurement data and that only systems granted full authorization to operate should be considered in reporting the number of systems certified and accredited. Clarification of such issues in future FISMA guidance would improve consistency and comparability of agency-reported FISMA information.

In analyzing these and future results indicated by agency-reported percentages of systems authorized after certification and accreditation, it is also important to consider several factors that lessen the usefulness of performance measurement data being reported by the agencies for FISMA.

As first discussed in our March 2004 testimony,[17] these factors include the following:

- *Limited assurance of data reliability and quality.* The FISMA performance measures reported by the agencies are primarily based on self-assessments and are not independently validated. OMB did not require IGs to validate agency responses to the performance measures, but did instruct them to assess the reliability of the data for the subset of systems they evaluate as part of their independent evaluations. Nonetheless, some IG evaluations did identify problems with data reliability and quality that could affect agency performance data. For example, for the performance measurement on the number of agency systems authorized for processing after certification and accreditation, six IGs indicated different results from those reported by their agencies, for reasons such as out-of-date certifications and accreditations. Further, as we discuss later in more detail, other IGs identified problems with the quality of the certifications and accreditations, such as security control reviews not being performed. OMB's requirement for IGs to assess the reliability of such information as part of their FISMA responsibilities could provide valuable information on the quality of reported FISMA information and assist management and Congress in their FISMA oversight. For example, for certifications and accreditations for the subset of systems they review, the IGs could determine whether the agencies met specific criteria, including a current risk assessment and security plan, control testing, and contingency planning and determine whether such information is accurately reflected in the agencies' compilation of related performance measures.

- *Accuracy of agency system inventories*. The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. However, according to their fiscal year 2003 FISMA reports, only 13 of the 24 agencies reported that they had completed their system

[17]GAO-04-483T.

inventories. Further, independent evaluations by IGs for 3 of these 13 agencies did not agree that system inventories were complete. Although we recently reported that all 24 agencies now report they develop and maintain the FISMA-required inventory of major information systems,[18] maintaining an accurate inventory will continue to be a key element of agency performance measures and in ensuring that information security programs cover all agency systems.

- *Further refinement of performance measures*. Refinement of FISMA performance measurement data is needed to provide better information on the status of agencies' information security efforts. For example, OMB currently requires agencies to report performance data in aggregate for the total number of agency systems, but does not require information that could be used to better assess the quality of certifications and accreditations performed, such as reporting systems according to their risk or security category, which would help indicate whether agencies are prioritizing their efforts according to risk and focusing on their most important systems. All the agencies responding to our survey indicated that they did prioritize their certification and accreditation efforts to focus on their most important systems. However, during our review of certifications and accreditations processes at the four agencies we visited, we noted that system prioritization was not always used to monitor overall activity. In fact, at one agency, system priority was not indicated in its overall inventory of systems, and one system identified by the agency as a national critical asset for critical infrastructure protection purposes had not been certified and accredited.[19] The agency has since acted to certify and accredit this system, recently reporting its full accreditation as of June 2004. OMB has also recognized the need for further information on agencies' certification and accreditation processes. According to its fiscal year 2003 report to the Congress, in fiscal year 2004 FISMA guidance, OMB planned to further emphasize security performance measurement, including evolving performance measures to move beyond status reporting to also identify the quality of the work done,

[18]U.S. General Accounting Office, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

[19]Critical infrastructure protection activities called for in federal policy and law are intended to enhance the security of cyber and physical, public and private infrastructures that are essential to national security, national economic security, or national public health and safety.

such as determining both the number of systems certified and accredited and the quality of certification and accreditation conducted.

Processes at Selected Agencies Do Not Ensure Consistent or Adequate Information

Although agencies responding to our survey indicated that their certification and accreditation processes required that specific criteria identified in federal guidance be met, our review of certification and accreditation documentation for selected systems at four agencies, as well as IG FISMA evaluations for fiscal year 2003, noted instances in which agencies do not consistently meet such criteria as a current risk assessment and security control evaluation. Further, three of the four agencies we reviewed had no routine processes to ensure that such criteria are met. In describing their processes, agencies identified challenges and obstacles to implementing an effective certification and accreditation program, such as resource and staffing constraints. They also identified successful practices to help mitigate such challenges.

Agencies Report Using Consistent Criteria

Agency responses to our survey showed that their certification and accreditation processes were generally consistent in how they defined system boundaries for certification and accreditation, with all 24 agencies reporting that they identified systems using OMB's definitions of a general support system and a major application. In addition, essentially all the agencies reported that their certification and accreditation processes for both new and existing systems required documentation or evidence to show that specific criteria found in federal guidance are met, such as requiring a current risk assessment and a security control evaluation. However, in one area—contingency plan testing—4 agencies (17 percent) reported that their processes did not require documentation that plans were tested. Two of these agencies reported that contingency plan testing was not required because either they thought it was inappropriate for new systems or their security program did not require such testing.[20] Table 2

[20]According to the National Institute of Standards and Technology's Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (June 2002), elements of contingency planning should be undertaken throughout the system development life cycle, including the development phase. Regarding testing, the guide notes that during the implementation phase for a new system, contingency strategies should be tested to ensure that technical features and recovery procedures are accurate and effective. Further, during the operations and maintenance phase of the system, exercises and tests should be conducted to ensure that the contingency plan procedures continue to be effective.

summarizes the agency responses for specific certification and accreditation criteria.

Table 2: Certification and Accreditation Criteria Required to Be Met by Processes at 24 Major Agencies

	Agency Responses	
Criterion	**Yes**	**No**
Current risk assessment?	24	0
Current security plan updated to reflect certification results?	23	1
Evaluated and documented management, operational, and technical security controls/requirements?	23	1
A plan with milestones prepared to correct weaknesses identified during security control evaluation?	24	0
Written management authorization that details the rules of behavior for systems that interface/interconnect with other agencies or contractors?	23	1
A current and adequate contingency plan?	22	2
System contingency plan has been tested?	20	4
Results of certification tests attested to by the certifier?	22	2
Residual risk identified by the certifier?	23	1
Specific corrective actions identified and recommended by the certifier?	22	2
An accreditation statement authorizing the system to process information and signed by the authorizing official?	23	1
An accreditation statement that indicates the level of residual risk being accepted by the authorizing official?	23	1
Authorizing official is a management official with general responsibility for the organizational mission supported by the system?	22	2

Source: Agency responses to GAO survey.

Processes at Selected Agencies Do Not Ensure that Criteria Are Met

Although the 24 agencies reported that they require specific criteria to be met, our analyses of documentation at 4 agencies for the certification and accreditation of a total of 32 mission- or national-critical systems showed that such documentation did not always demonstrate that specific criteria were met. For example, only 22 of the 32 systems showed results of control testing and only 19 systems had contingency plans. In addition, documentation for only 17 of the systems identified the actual residual risk being accepted by the accrediting official. Table 3 summarizes results for these and other criteria for the agencies.

Table 3: Number and Percentage of 32 Selected Agency Systems Meeting Specific Certification and Accreditation Criteria

Criterion	Number of systems meeting criterion (percentage)	
Current risk assessment?	23	(72%)
Current security plan?	26	(81%)
Controls tested?	22	(69%)
Contingency plan?	19	(59%)
Contingency plan tested?	8	(42%)[a]
Plan with milestones prepared for weaknesses?	17	(81%)[b]
Residual risk identified?	17	(53%)

Source: GAO analysis of agency data.

[a]Percentage based on the total of 19 systems with contingency plans.

[b]Percentage based on 21 systems for which plans were required to correct identified weaknesses.

As we recently testified, results of IG FISMA independent evaluations have also demonstrated deficiencies in agencies' certifications and accreditations.[21] Some of their fiscal year 2003 FISMA reports identified instances in which certifications and accreditations were not current and controls were not tested. Others also recommended improvements in agency processes. For example, for the Office of Personnel Management, the IG recommended that the agency develop a procedure to ensure that all documented findings and corrective actions are reviewed by both the certification and accreditation officials and included in the certification statement, accreditation statement, and plan of action and milestones report.

At the four agencies we reviewed, only the IGs at Commerce and Energy specifically addressed certification and accreditation as part of their fiscal year 2003 FISMA reporting. The Commerce IG recognized that the department was undergoing changes in implementing new certification and accreditation guidance, but reported cases in which system certification was granted without evidence of testing. The Energy IG reported findings that included lack of security control reviews and management authorizations to operate systems, as well as risk assessments that were

[21]GAO-04-483T.

incomplete or outdated and system security plans that were missing critical elements or did not cover changes to their IT environment.

Lastly, CIO offices at the four agencies we reviewed monitored the status of system certifications and accreditations agencywide, but only one—Commerce—routinely assessed the quality of its efforts. Largely to facilitate FISMA reporting to OMB, the agencies all had processes to update the status of system certification and accreditation activities, ranging from periodic data calls at Energy to EPA's use of its Automated Security Self-Evaluation and Remediation Tracking tool to centrally track Web-enabled plans of action and milestones reports.[22] These processes do not ensure the quality of the certifications and accreditations, such as whether the criteria identified in guidance are met. Such a quality control process could facilitate accrediting officials consistently receiving sufficient information on which to base their decisions, yet only Commerce had an agencywide process to routinely ensure quality. As described by a Commerce IT security official, the department has a continuous, comprehensive control review process that includes annual program and system evaluations through both self-assessments by component program managers and compliance reviews by IT security officials under the Commerce CIO. Specifically with regard to certification and accreditation, the process includes the use of a checklist on the content and quality of the documentation. Further, as part of the compliance review process, in fiscal year 2003, Commerce conducted reviews to ensure that all the department's classified, mission-critical, and national-critical systems met legal and departmental requirements. These reviews included checks for compliance with certification and accreditation criteria, such as risk assessments, contingency plans, certifier's statements, and accreditation letters. According to the Commerce official, such reviews will continue to be conducted on a sample basis with all systems reviewed at least once over a 3-year review cycle. An official at Energy also identified a process to independently verify and validate that department's certification and accreditation packages, but explained that due to the large number of systems, this process has been limited to reviews for its headquarters systems. This official added that to help address this issue, they are

[22]ASSERT is an Internet-based, automated version of NIST's *Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26) that annually evaluates the risk in computer systems at EPA and produces and centrally tracks Web-enabled plans of action and milestones reports.

working with the IG's office to have it begin conducting random reviews of certification and accreditation packages this fall.

Challenges and Obstacles to Agency Processes

Through our survey and interviews with agency staff, agencies noted several overall challenges or obstacles to efforts to certify and accredit their systems. Funding and staffing issues were most commonly indicated, including those associated with implementing the new NIST guidance.

According to OMB's March 2004 report to the Congress, funding for IT security has increased from $2.7 billion in FY 2002 to $4.2 billion in FY 2003. Nevertheless, a total of 18 agencies identified funding as a challenge to performing their certifications and accreditations. For example, Commerce noted that certification and accreditation was an expensive process and that in order to develop and implement its program, it had to reprogram and reprioritize internal funds and absorb costs in existing funding levels. In another case, the Department of Health and Human Services stated that because of limited funding, higher emphasis is placed on using funds to certify and accredit new systems as opposed to existing systems. Energy also noted that funding was a challenge because security costs were not integrated into the overall life-cycle costs for all of its systems. Despite these and other concerns related to security cost funding, most agencies did not know how much they spent on certification and accreditation. For example, only 11 agencies could identify their actual or estimated costs for fiscal year 2003, which totaled $75.5 million for these agencies.

Nineteen of the agencies we surveyed also reported that they had encountered staffing challenges for their certification and accreditation activities that essentially consisted of the need for full-time staff with the appropriate backgrounds, specialized skills, and security clearances. In addition, 13 agencies reported challenges in providing training to staff or officials responsible for certifying or accrediting agency systems.

In Special Publication 800-37, NIST acknowledges that the cost of conducting certifications and accreditations on large numbers of information systems with varying degrees of complexity is a critical issue facing agencies today. NIST suggests part of the solution is promoting the reuse and sharing of security control development, implementation, and assessment-related information in the agency's agencywide information security program, including

- employment of standardized security controls and methods for assessing those controls;

- development of standardized assessment plans, methods and procedures to be used in security certifications and accreditations;

- adoption, specification, and promulgation of standardized policies, procedures, and documentation for common security program areas (e.g., rules of behavior, system administration, auditing, system monitoring, vulnerability scanning, management of user accounts, configuration management, incident response, contingency planning, and system maintenance);

- refinement of policies, procedures, and documentation on a system-by-system basis, as needed, by preparing amendments or adding system-specific appendixes;

- adoption, publication, and distribution (preferably in an online database) of agency-prescribed or -developed security implementation guidance;

- establishment of a protected central repository, preferably online, for all certification and accreditation documentation, acquisition-related information, risk and vulnerability assessments, compliance surveys, security incident reporting and remediation results, external security audits, and making these easily accessible by appropriate agency personnel; and

- procurement of agencywide licenses for automated tools such as vulnerability scanners, online security monitoring tools, audit reduction tools, and certification and accreditation support tools.

As another means to help address the cost of certification and accreditation, the NIST guideline also highlights the importance of leveraging the results of previous assessments and audits conducted on an agency's information system or the particular products comprising that system. Potential sources identified include commercial product testing and evaluation programs, privacy impact assessments, physical security assessments, self-assessments, and internal and external audits. According to the guideline, these assessments and audits can support the security certification and accreditation process by helping to gauge the preparedness of an information system for security certification and

accreditation by examining the status of key security controls in the system and by potentially being reused as evidence, when appropriate, during the security certification and accreditation process. Further, evidence from other assessments and audits can help reduce the potential cost of security certification and accreditation, as well as increase the overall confidence in the final certification and accreditation results.

Although the NIST guideline emphasizes leveraging the results of previous assessments and audits, it is important that agencies note the difference between the level of control testing envisioned for annual FISMA testing and that performed for system certification and accreditation. FISMA requires agencies to periodically test and evaluate the effectiveness of information security policies, procedures, and practices for each system with a frequency depending on risk, but no less than annually. In contrast, current OMB policy requires agencies to reaccredit their systems (which also includes control testing) at least every 3 years. In its fiscal year 2003 FISMA reporting guidance, OMB distinguished between these two requirements, explaining that annual FISMA testing is not of the complexity required for certification and accreditation of systems as described in NIST guidance. Rather, the FISMA provision recognizes the importance of maintaining a continuous process of assessing risk and ensuring that security controls maintain risk at an acceptable level and underscores the need to understand the security status of each system in order to accurately maintain system-level plans of action and milestones and report annually on the overall health of an agency's IT security program.

During our review, agencies also identified some actions that can help address identified challenges and contribute to more efficient and effective certification and accreditation processes. In particular, citing proactive senior management support as critical to the success of its program, Commerce identified several actions, including that it has

- informed program mangers of their responsibilities and held them accountable for the security of IT resources;
- redefined system boundaries to better organize certification and accreditation efforts and manage systems;
- collaborated to solve common obstacles and to optimize available internal departmental resources both in the central security program office and in other bureaus to overcome skills gaps and staff shortages;

- provided role-based training that tailors certification and accreditation requirements and responsibilities to those with IT security roles; and

- reviewed mission critical and national critical systems to ensure that they are in compliance with the department's security policy and guidance.

Other identified actions included those by Transportation, which maintains a dedicated, trained, experienced staff of contractors as part of its centralized certification process and provides training to system owners during the certification process. In addition, as mentioned previously, EPA has developed a tool to annually evaluate the risk in computer systems and to produce and centrally track Web-enabled plans of action and milestones reports. EPA is offering this tool to other agencies, including hosting the tool for them at its National Computer Center. Lastly, 21 of the 24 agencies surveyed reported that they used automated tools as part of their certification and accreditation process for a number of functions, including managing the process and developing documentation, tracking corrective actions, configuration management, vulnerability scanning, penetration testing, and technical controls testing.

Conclusions

Certification and accreditation has become a key measure in determining the status of agencies' information security programs, and NIST and other agencies have provided overall guidance to assist agencies in establishing effective certification and accreditation. Agencies are reporting increasing numbers of systems certified and accredited, but some still have not certified a significant percentage of their systems. Further, agency certifications and accreditations do not always meet criteria identified in federal guidance. Unless such criteria are met, agencies cannot ensure that accrediting officials are receiving consistent information on which to base their decisions, and the value of this process as a management control for ensuring information system security is limited. In addition, unverified agency-reported performance data may not accurately reflect the status of an agency's efforts to implement this requirement. Consistent reporting of performance measurement data by agencies on their certifications and accreditations, as well as additional information on the quality of agency processes provided through both management oversight and independent evaluation, would provide increased assurance for the administration and the Congress that critical federal systems are meeting FISMA requirements and do not contain significant security weaknesses that could threaten essential federal operations. It would also assist the administration and the

Congress in their oversight responsibilities by helping to identify and respond to challenges in effectively and efficiently implementing this requirement for the federal government.

Recommendations for Executive Action

To help ensure that federal agencies' certification and accreditation processes consistently provide adequate and effective security controls in their information systems, we recommend that the Director of the Office of Management and Budget take the following five actions. First, we recommend that the OMB Director revise policy and guidance on the security of automated information resources to require federal agencies to

- continue to implement security certification and accreditation processes consistent with guidance and standards issued by NIST for non-national security systems, including specific reference to the new certification and accreditation guidance as well as FISMA-required standards such as those for system security categorization and minimum security controls; and

- ensure that periodic testing and evaluation of information security controls, as required by FISMA, include assessing the quality of security certifications and accreditations to facilitate decisions that are based on consistent consideration of key criteria outlined in federal guidance, including a current risk assessment, appropriate control testing and evaluation, a tested contingency plan, and the identification of the specific residual risk being accepted.

Further, to improve the consistency and reliability of agency FISMA reporting for administration and congressional oversight, we recommend that the OMB Director consider changes to OMB's FISMA reporting guidance that would

- provide additional clarification that national security systems are to be reflected in reporting performance measurement data and that only systems granted full authorization to operate should be considered in reporting the number of systems certified and accredited;

- require reporting on key aspects of agencies' certification and accreditation processes and efforts, such as how agencies ensure the quality and consistency of their certifications and accreditations and the status of their efforts according to levels of risk or impact established for their systems; and

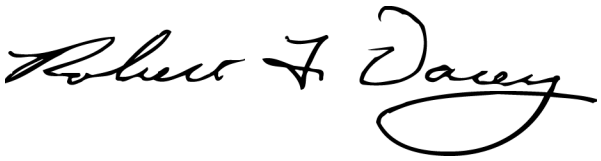
- encourage the IGs to assess agency FISMA reporting processes and test agency-reported performance data as part of their FISMA-mandated independent evaluations; for example, the IGs could review the quality of agency certifications and accreditations for the subset of systems they evaluate to determine whether they meet appropriate criteria and determine whether such information is accurately reflected in the agencies' compilation of related performance measures.

Agency Comments

We received oral comments on a draft of this report from representatives of OMB's Office of Information and Regulatory Affairs and Office of General Counsel. The representatives agreed with our findings that the quality of agency certification and accreditation processes varies, and generally agreed with our recommendations to improve certification and accreditation processes. OMB stated that it plans to address key certification and accreditation practices in its upcoming FISMA reporting guidance to agencies, and believes the recent completion of NIST Special Publication 800-37 and reviews by designated accrediting authorities are fundamental drivers for improving the quality of the certification and accreditation process. In addition, OMB stated its belief that existing guidance, including its Circular A-130 and FISMA implementing guidance, helps ensure that implementation of certification and accreditation is effective, and that its planned agency guidance for fiscal year 2004 FISMA reporting will address many of the issues in our report. The Department of Commerce provided written comments on a draft of this report (see app. I). In these comments, the department generally agreed with our report and provided certain technical comments. We also received written and oral technical comments from the Departments of Defense and Energy, EPA, NASA, and NIST. Comments from all these agencies have been incorporated into the report, as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it 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 heads of the agencies discussed in the report. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov. Copies will also be made available to others upon request.

Should you or your offices have any questions concerning this report, please call me at (202) 512-3317 or Ben Ritt, Assistant Director, at (202) 512-6443. We can also be reached by e-mail at daceyr@gao.gov and rittw@gao.gov, respectively. Key contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Information Security Issues

Comments from the Department of Commerce

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

June 23, 2004

Mr. Robert F. Dacey
Director, Information Security Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. Dacey:

Thank you for the opportunity to comment on the GAO draft report "Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation." The report presents a realistic representation of the state of certification and accreditation (C&A) practices in the Federal Government today, and the information attributed to the Department of Commerce is accurate, except as noted in the enclosure.

The Department of Commerce recognizes the value of establishing sound, repeatable, consistent practices to ensure the quality of the C&A process for federal information technology (IT) systems. We appreciate the support of Congress and OMB for establishing requirements for these practices, and are pleased with GAO's recognition of the National Institute of Standards and Technology (NIST) as it provides comprehensive federal guidance in this important area.

We have accorded IT security a high priority in the Commerce Department, and are also pleased to support other federal agencies and the private sector through our NIST IT security products.

Sincerely,

Donald L. Evans

Enclosure

GAO Contact and Staff Acknowledgments

GAO Contact

William B. Ritt, (202) 512-6443

Acknowledgments

In addition to the person named above, Larry Crosland, Mark Fostek, Michael P. Fruitman, Danielle Hollomon, Elizabeth Johnston, Anjalique Lawrence, Min Lee, Tracy Pierson, and Monica Wolford made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

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

Order by Mail or Phone

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

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00