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.