G A O
Accountability•Integrity•Reliability
Highlights

Highlights of GAO-04-483T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Goverment Reform

March 16, 2004

INFORMATION SECURITY

Continued Efforts Needed To Sustain Progress in Implementing Statutory Requirements

Why GAO Did This Study

For many years, GAO has reported on the widespread negative impact of poor information security within federal agencies and has identified it as a governmentwide high-risk issue since 1997. Legislation designed to improve information security was enacted in October 2000. It was strengthened in December 2002 by new legislation, the Federal Information Security Management Act of 2002 (FISMA), which incorporated important new requirements.

This testimony discusses

- the Office of Management and Budget's (OMB) recent report to the Congress required by FISMA on the government's overall information security posture,
- the reported status of efforts by 24 of the largest agencies to implement federal information security requirements,
- opportunities for improving the usefulness of performance measurement data, and
- progress by the National Institute of Standards and Technology (NIST) to develop related standards and guidance.

www.gao.gov/cgi-bin/getrpt?GAO-04-483T.

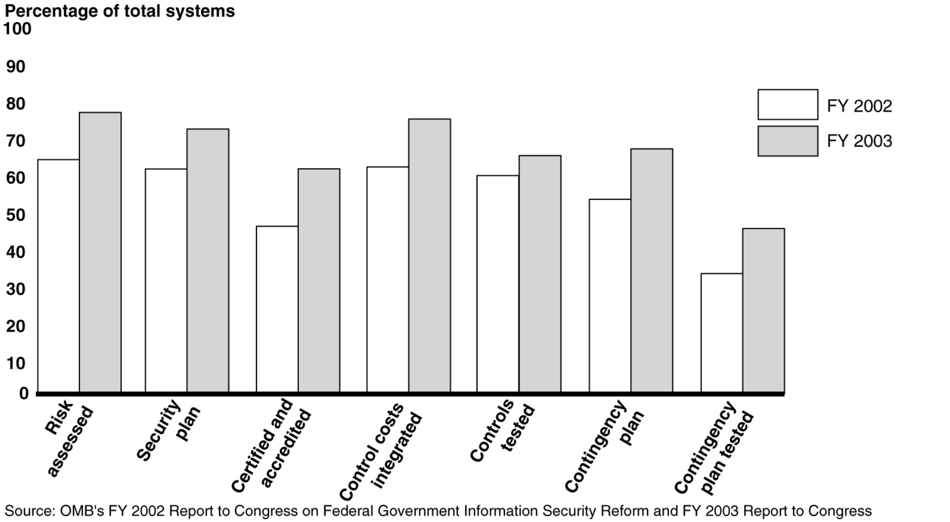
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

OMB reports significant strides in addressing long-standing problems, but at the same time cites challenging weaknesses that remain. One governmentwide weakness OMB emphasizes is a lack of understanding—and therefore accountability—on the part of agency officials regarding their responsibilities for ensuring the security of information and systems. The report presents a plan of action to close these gaps through both management and budgetary processes.

Fiscal year 2003 FISMA data showed that, overall, the 24 federal agencies reported increasing numbers of their systems met the information security requirements represented by key OMB performance measures. For example, of the total number of systems reported by these agencies, the reported number assessed for risk climbed from 65 percent to 78 percent, those having a contingency plan jumped from 55 to 68 percent, and those authorized for processing following certification and accreditation rose from 47 to 62 percent (see chart). However, reported results varied widely among individual agencies, with some reporting that less than half of their systems met certain requirements. Further, GAO noted opportunities to improve the usefulness of reported performance management data, including independent validation of these data and completion of system inventories.

Reported Performance Measurement Data for Selected Information Security Requirements for 24 Large Federal Agencies



Source: OMB's FY 2002 Report to Congress on Federal Government Information Security Reform and FY 2003 Report to Congress on Federal Government Information Security Management; GAO (analysis).

NIST made progress in developing security-related standards and guidance required by FISMA. These include standards to categorize systems according to potential impact in the event of a security breach and recommended controls for such systems. However, according to NIST, current and future funding constraints could threaten its information security work.