June 24, 2003

INFORMATION SECURITY

Continued Efforts Needed to Fully Implement Statutory Requirements

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-852T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

Why GAO Did This Study

Since 1996, GAO has reported that poor information security in the federal government is a widespread problem with potentially devastating consequences. Further, GAO has identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003. To strengthen information security practices throughout the federal government, information security legislation has been enacted.

This testimony discusses efforts by federal departments and the administration to implement information security requirements mandated by law. In so doing, it examines

- overall information security weaknesses and challenges that the government faces, and the status of actions to address them, as reported by the Office of Management and Budget (OMB);
- GAO's evaluation of agency efforts to implement federal information security requirements and correct identified weaknesses; and
- new requirements mandated by the Federal Information Security Management Act of 2002 (FISMA).

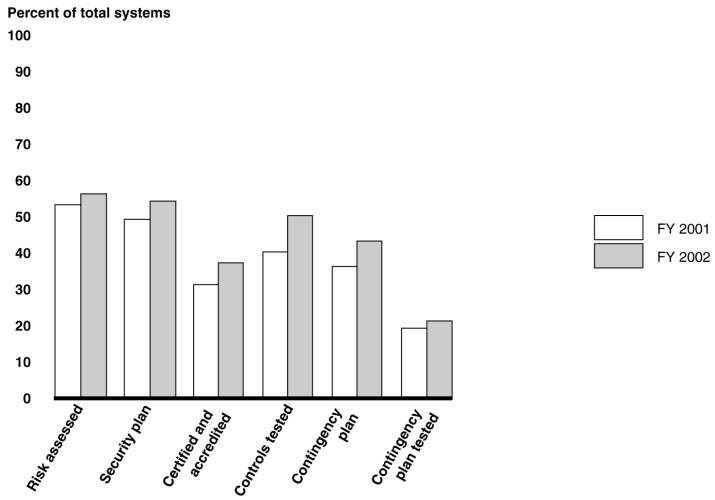
What GAO Found

Based on the fiscal year 2002 reports submitted to OMB, the federal government has made limited overall progress in implementing statutory information security requirements, although a number of benefits have resulted. Among these benefits are several actions taken and planned to address governmentwide information security weaknesses and challenges, such as lack of senior management attention. Nevertheless, as indicated by selected quantitative performance measures for the largest federal agencies, progress has been limited. Specifically, excluding data for one agency that were not comparable for fiscal years 2001 and 2002, improvements for 23 agencies ranged from 3 to 10 percentage points for the selected measures (see figure).

GAO's analyses of agencies' reports and evaluations confirmed that many agencies have not implemented security requirements for most of their systems, such as performing risk assessments and testing controls. Further, the usefulness of agency corrective action plans may be limited when they do not identify all weaknesses or contain realistic completion dates. Agencies also continue to face challenges in effectively implementing and managing their overall information security programs.

FISMA provisions establish additional requirements that, among other things, can assist agencies in implementing effective information security programs. However, attaining significant and sustainable results in implementing such requirements will also likely require processes that prioritize and routinely monitor and manage agency efforts, as well as continued congressional and administration oversight.

Performance Measure Percentages for Selected Information Security Requirements[a]



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform and GAO (analysis).

[a]Excludes National Aeronautics and Space Administration data.

www.gao.gov/cgi-bin/getrpt?GAO-03-852T.

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.