April 2005

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-05-483T, a testimony before the House Committee on Government Reform.

Why GAO Did This Study

For many years, GAO has reported that poor information security is a widespread problem that has potentially devastating consequences. Further, since 1997, GAO has identified information security as a governmentwide high-risk issue in reports to Congress—most recently in January 2005.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

This testimony discusses:

- The federal government's progress and challenges in implementing FISMA as reported by the Office of Management and Budget (OMB), the agencies, and Inspectors General (IGs).
- Opportunities for improving the usefulness of the annual reporting process, including the consideration of a common framework for the annual FISMA reviews conducted by the IGs.

www.gao.gov/cgi-bin/getrpt?GAO-05-483T.

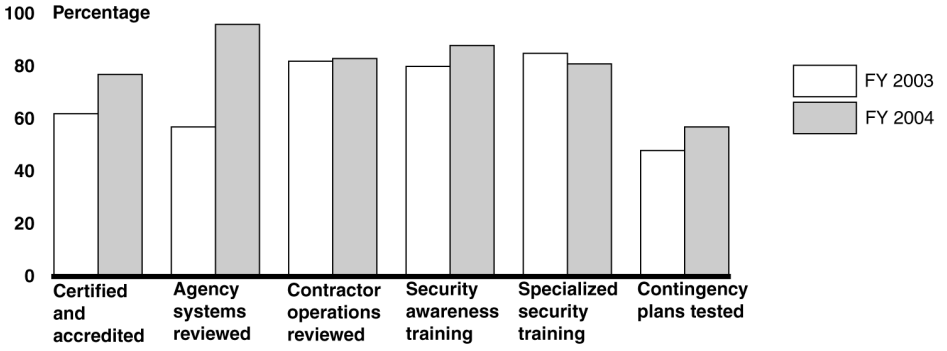
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-3317 or wilshuseng@gao.gov.

What GAO Found

In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long-standing problems, but at the same time, cites challenging weaknesses that remain. The report notes several governmentwide findings, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation (the process of authorizing operation of a system including the development and implementation of risk assessments and security controls). Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003 (see figure). Nevertheless, challenges remain. For example, only 7 agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and 6 of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems.

Opportunities exist to improve the usefulness of the annual FISMA reporting process, including enhancing the reliability and quality of reported information, providing performance information based on the relative importance or risk of the systems, and reporting on key information security requirements. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.

Percentage of Selected Performance Measurement Data for 24 Federal Agencies



Source: OMB's FY2003 and 2004 Report to Congress on Federal Government Information Security Management; GAO (analysis).