April 14, 2005

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-567T, a testimony before the House Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security

INFORMATION SECURITY

Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements

Why GAO Did This Study

For many years, GAO has reported that poor information security is a widespread problem that has potentially devastating consequences. Accordingly, 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 made 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. FISMA requires that agencies report annually to OMB who issues guidance for that reporting process.

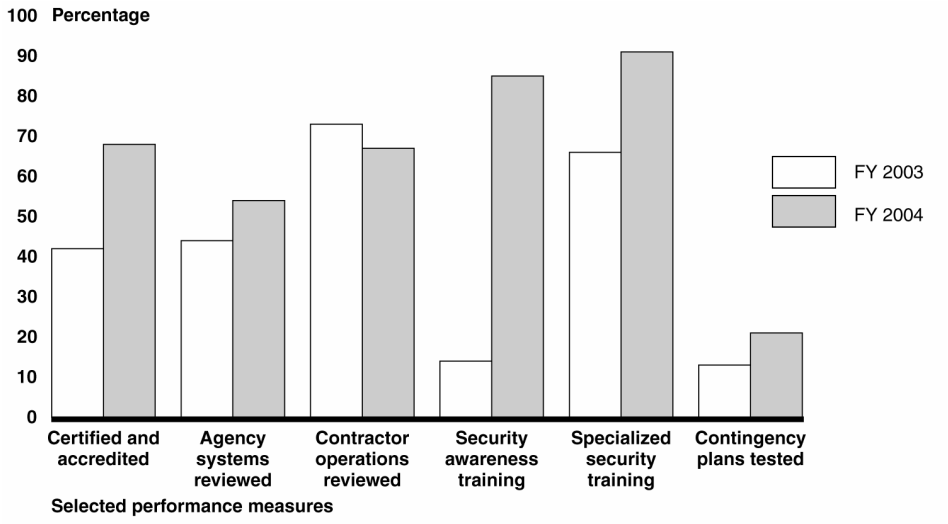
The Department of Homeland Security (DHS), the third largest agency in the federal government, uses a variety of major applications and general systems in support of operational and administrative requirements.

This testimony discusses DHS's progress and challenges in implementing FISMA as reported by the agency and its Inspector General (IG).

What GAO Found

DHS has made progress in implementing key federal information security requirements, yet it continues to face challenges in fulfilling the requirements mandated by FISMA. In its fiscal year 2004 report on FISMA implementation, DHS highlights increases in the majority of the key performance measures (developed by the Office of Management and Budget (OMB) to track agency performance in implementing information security requirements), such as the percentage of agency systems reviewed and percentage of employee and contractor personnel who received security awareness training (see figure). For example, DHS reported a substantial increase in the percentage of personnel that received security awareness training, rising from 14 percent in fiscal year 2003 to 85 percent in fiscal year 2004. However, DHS continues to face significant challenges in meeting most statutory information security requirements. For example, DHS has yet to develop a complete and accurate inventory or an effective remediation process.

Figure: DHS Performance Data for Key OMB Performance Measures



Sources: DHS' FY2003 and FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

www.gao.gov/cgi-bin/getrpt?GAO-05-567T.

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.