GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-837, a report to congressional committees

July 2007

INFORMATION SECURITY

Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem with potentially devastating consequences—such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information—and has identified information security as a governmentwide high-risk issue.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies.

As required by FISMA to report periodically to Congress, in this report GAO discusses the adequacy and effectiveness of agencies' information security policies and practices and agencies' implementation of FISMA requirements. To address these objectives, GAO analyzed agency, inspectors general (IG), Office of Management and Budget (OMB), congressional, and GAO reports on information security.

What GAO Recommends

GAO is recommending that OMB strengthen FISMA reporting metrics. OMB agreed to take GAO's recommendations under advisement when modifying its FISMA reporting instructions.

www.gao.gov/cgi-bin/getrpt?GAO-07-837.

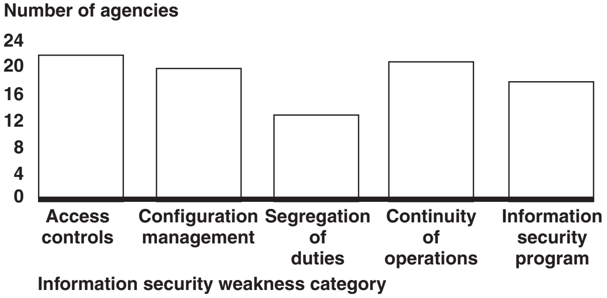
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Significant weaknesses in information security policies and practices threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. Recently reported incidents at federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to loss of privacy and identity theft. Almost all of the major federal agencies had weaknesses in one or more areas of information security controls (see figure). Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer resources. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; or maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully implemented their information security programs. As a result, agencies may not have assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006, agencies generally reported performing various control activities for an increasing percentage of their systems and personnel. However, IGs at several agencies disagreed with the information the agency reported and identified weaknesses in the processes used to implement these activities. Further, although OMB enhanced its reporting instructions to agencies for preparing fiscal year 2006 FISMA reports, the metrics specified in the instructions do not measure how effectively agencies are performing various activities, and there are no requirements to report on a key activity. As a result, reporting may not adequately reflect the status of agency implementation of required information security policies and procedures.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis of IG, agency, and GAO reports.