June 7, 2007

INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-935T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

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.

In this testimony, GAO discusses security incidents reported at federal agencies, the continued weaknesses in information security controls at major federal agencies, agencies' progress in performing key control activities, and opportunities to enhance FISMA reporting and independent evaluations. To address these objectives, GAO analyzed agency, inspectors general (IG), and GAO issued and draft reports on information security.

www.gao.gov/cgi-bin/getrpt?GAO-07-935T.

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

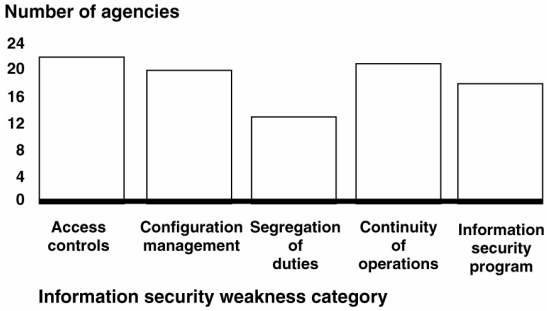
What GAO Found

Federal agencies have recently reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscore the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. 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 networks, systems, or information. For example, agencies did not consistently identify and authenticate users to prevent unauthorized access, apply encryption to protect sensitive data on networks and portable devices, and restrict physical access to information assets. 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; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. However, IGs at several agencies sometimes disagreed with the agency's reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis.