July 2005

INFORMATION SECURITY

Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-552, a report to congressional committees

Why GAO Did This Study

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on 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 (FISMA) in 2002.

In accordance with FISMA requirements that the Comptroller General report periodically to the Congress, GAO's objectives in this report are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the federal government's implementation of FISMA requirements.

What GAO Recommends

GAO recommends that the Director of the Office of Management and Budget (OMB) implement improvements in the annual FISMA reporting guidance. In commenting on a draft of this report, OMB agreed with GAO's overall assessment of information security at agencies but disagreed with aspects of our recommendations to enhance its FISMA reporting guidance.

www.gao.gov/cgi-bin/getrpt?GAO-05-552.

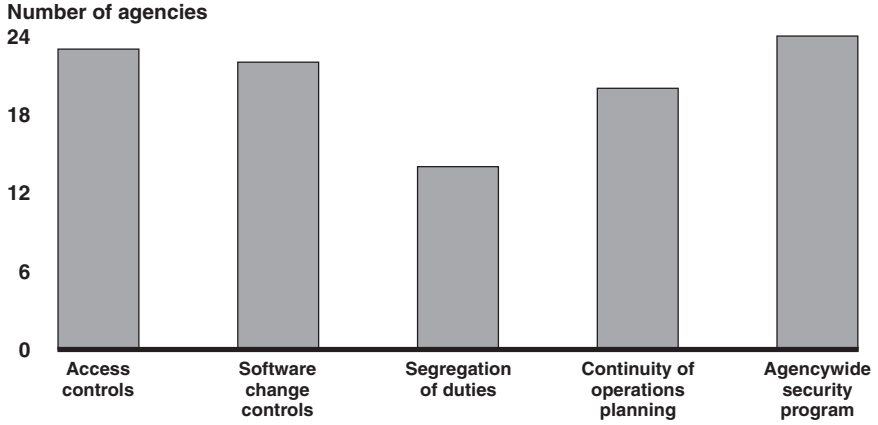
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Pervasive weaknesses in the 24 major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of federal information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; continuity of operations planning was often inadequate; and security programs were not fully implemented at the agencies (see figure). These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Overall, the government is making progress in its implementation of FISMA. To provide a comprehensive framework for ensuring the effectiveness of information security controls, FISMA details requirements for federal agencies and their inspectors general (IG), the National Institute of Standards and Technology (NIST), and OMB. Federal agencies reported that they have been increasingly implementing required information security practices and procedures, although they continue to face major challenges. Further, IGs have conducted required annual evaluations, and NIST has issued required guidance in the areas of risk assessments and recommended information security controls, and has maintained its schedule for issuing remaining guidance required under FISMA. Finally, OMB has given direction to the agencies and reported to Congress as required; however, GAO's analysis of its annual reporting guidance identified opportunities to increase the usefulness of the reports for oversight. While progress has been made in implementing statutory requirements, agencies continue to have difficulty effectively protecting federal information and information systems.

Information Security Weaknesses at the 24 Major Agencies



Source: GAO.