May 19, 2009

INFORMATION SECURITY

Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-701T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Without proper safeguards, federal agencies' computer systems are vulnerable to intrusions by individuals and groups who have malicious intentions and can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Concerned by reports of significant weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on its draft report on (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) their implementation of FISMA requirements. To prepare for this testimony, GAO summarized its draft report where it analyzed agency, inspectors general, Office of Management and Budget (OMB), congressional, and GAO reports on information security.

What GAO Recommends

In its draft report, GAO is recommending that the Director of OMB take several actions, including revising guidance.

View GAO-09-701T or key components. 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 expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. GAO's audits and reviews by inspectors general note significant information security control deficiencies that place agency operations and assets at risk. In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that the information system controls over their financial systems and information were either a significant deficiency or a material weakness. In addition, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. Twenty-three of the 24 major federal agencies had weaknesses in their agencywide information security programs.

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. For fiscal year 2008 reporting, agencies reported higher levels of FISMA implementation for most information security metrics and lower levels for others. Increases were reported in the number and percentage of employees and contractors receiving security awareness training, the number and percentage of systems with tested contingency plans, and the number and percentage of systems that were certified and accredited. However, the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly and the number and percentage of systems that had been tested and evaluated at least annually decreased slightly. In addition, the current reporting instructions do not request inspectors general to report on agencies' effectiveness of key activities and did not always provide them with clear guidance for annual reporting. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices. Without such information, Congress may not be fully informed about the state of federal information security.