G A O
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-496T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Information security is especially important for federal agencies, where the public's trust is essential and poor information security can have devastating consequences. Since 1997, GAO has identified information security as a governmentwide high-risk issue in each of its biennial reports to the Congress. Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on the current state of federal information security and compliance with FISMA. This testimony summarizes (1) agency progress in performing key control activities, (2) the effectiveness of information security at federal agencies, and (3) opportunities to strengthen security. In preparing for this testimony, GAO reviewed prior audit reports; examined federal policies, guidance, and budgetary documentation; and analyzed agency and inspector general (IG) reports on information security.

To view the full product, including the scope and methodology, click on GAO-08-496T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

February 14, 2008

INFORMATION SECURITY

Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies

What GAO Found

Over the past several years, federal agencies consistently reported progress in performing certain information security control activities. According to the President's proposed fiscal year 2009 budget for information technology, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by the Office of Management and Budget (OMB). The percentage of certified and accredited systems governmentwide reportedly increased from 88 percent to 92 percent. Gains were also reported in testing of security controls – from 88 percent of systems to 95 percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that GAO reported on last year.

Despite reported progress, major federal agencies continue to experience significant information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete 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. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by an increasing number of security incidents experienced by federal agencies.

Nevertheless, opportunities exist to bolster federal information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information systems security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.