March 12, 2008

INFORMATION SECURITY

Progress Reported, but Weaknesses at Federal Agencies Persist

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-571T, a testimony before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

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 our biennial reports to 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) the status of agency performance of information security control activities as reported by major agencies and their inspectors general (IG), (2) the effectiveness of information security at federal agencies, and (3) opportunities to improve federal information security. In preparing for this testimony, GAO analyzed agency, IG, Office of Management and Budget (OMB), and GAO reports on information security and reviewed OMB FISMA reporting instructions, information technology security guidance, and information on reported security incidents.

To view the full product, including the scope and methodology, click on GAO-08-571T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Over the past several years, 24 major federal agencies have consistently reported progress in performing information security control activities in their annual FISMA reports. For fiscal year 2007, the federal government continued to report improved information security performance relative to key performance metrics established by OMB. For example, an increasing percentage of systems governmentwide had been tested and evaluated, had tested contingency plans, and had been certified and accredited. However, IGs at several agencies sometimes disagreed with the agency reported information and identified weaknesses in the processes used to implement these and other security program activities.

Despite agency reported progress, major federal agencies continue to experience significant information security control deficiencies that limit the effectiveness of their efforts to protect the confidentiality, integrity, and availability of their information and information systems. 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 effectively 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.