May 5, 2009

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-661T, 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

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

GAO was asked to describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. To do so, GAO relied on its previous reports and reviewed agency and inspectors general reports on information security.

What GAO Recommends

In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-09-661T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal, and cyber exploitation activity has grown more sophisticated, more targeted, and more serious. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. In the absence of robust security programs, agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. These developments have led government officials to become increasingly concerned about the potential for a cyber attack.

According to GAO reports and annual security reporting, federal systems are not sufficiently protected to consistently thwart cyber threats. Serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. For example, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, and information, and weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. Agencies also did not always configure network devices and service properly, segregate incompatible duties, or ensure that continuity of operations plans contained all essential information. An underlying cause for these weaknesses is that agencies have not yet fully or effectively implemented key elements of their agencywide information security programs. To improve information security, efforts have been initiated that are intended to strengthen the protection of federal information and information systems. For example, the Comprehensive National Cybersecurity Initiative was launched in January 2008 and is intended to improve federal efforts to protect against intrusion attempts and anticipate future threats. Until such opportunities are seized and fully exploited and GAO recommendations to mitigate identified control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain vulnerable.