April 19, 2007

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-751T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem with potentially devastating consequences—such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information. In reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies. FISMA also defines responsibilities for ensuring centralized compilation and analysis of incidents that threaten information security and providing timely technical assistance in handling security incidents.

In this testimony, GAO discusses the continued weaknesses in information security controls at 24 major federal agencies, the reporting and analysis of security incidents, and efforts by the Department of Homeland Security (DHS) to develop a cyber threat analysis and warning capability.

GAO based its testimony on its previous work in this area as well as agency and congressional reports.

www.gao.gov/cgi-bin/getrpt?GAO-07-751T.

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.

INFORMATION SECURITY

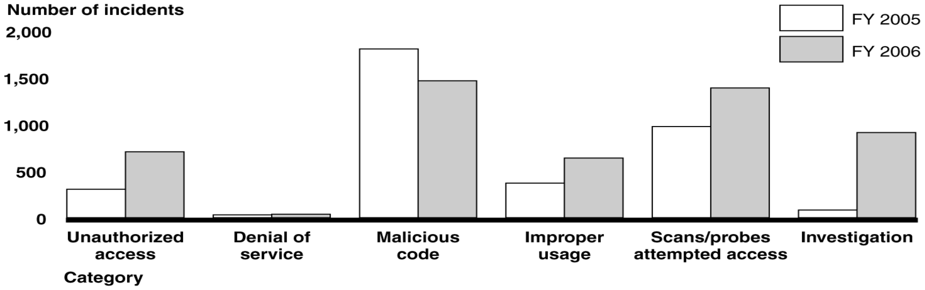
Persistent Weaknesses Highlight Need for Further Improvement

What GAO Found

In their fiscal year 2006 financial statement audit reports, 21 of 24 agencies indicated that they had significant weaknesses in information security controls. As shown by reports by GAO and agency inspectors general (IG), the weaknesses persist in major categories of controls—including, for example, access controls, which ensure that only authorized individuals can read, alter, or delete data, and configuration management controls, which provide assurance that only authorized software programs are implemented. An underlying cause for these weaknesses is that agencies have not yet fully implemented agencywide information security programs, which provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent unauthorized use, disclosure, and modification.

Organizations can reduce the risks associated with intrusions and misuse if they take steps to detect and respond to incidents before significant damage occurs, analyze the causes and effects of incidents, and apply the lessons learned. As part of this process, federal policy requires agencies to report incidents to the federal information security incident center—US-CERT (Computer Emergency Readiness Team). According to US-CERT, federal agencies reported a record number of incidents in fiscal year 2006. As the figure shows, since 2005, the number of incidents reported increased in every category except one. However, inconsistencies exist in reporting at various levels. If agencies do not properly capture and analyze security incidents, they risk losing valuable information needed to prevent future exploits and understand the nature and cost of security threats.

Strategic analysis and warning is an essential element of assisting agencies in addressing information security incidents. GAO has recommended that DHS develop such a capability for addressing cyber attacks. DHS has established various initiatives to enhance its analytical capabilities through US-CERT and GAO believes with continued progress in addressing strategic analysis and warnings, US-CERT can further agencies' efforts to reduce risks associated with incidents.



Source: GAO analysis of OMB data.