March 24, 2010

INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-536T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives

Why GAO Did This Study

Without proper safeguards, federal computer systems are vulnerable to intrusions by individuals who have malicious intentions and can obtain sensitive information. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained cyber attacks against the United States; these attacks continue to pose a potentially devastating impact to systems as well as the operations and critical infrastructures that they support. Concerned by reports of weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on federal information security and agency efforts to comply with FISMA. This testimony summarizes (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. To prepare for this testimony, GAO analyzed its prior reports and those from 24 major federal agencies, their inspectors general, and the Office of Management and Budget (OMB).

What GAO Recommends

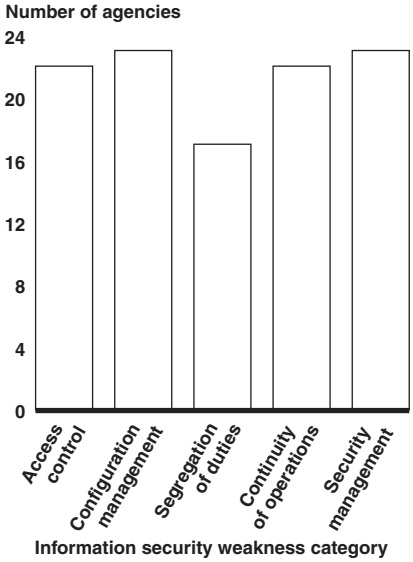
In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-10-536T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have reported mixed progress in securing their systems and implementing key security activities. For example, in fiscal year 2009, agencies collectively reported an increasing percentage of personnel receiving security awareness training and specialized security training, but a decreasing rate of implementation for other key activities when compared to fiscal year 2008. In addition, federal systems continued to be afflicted by persistent control weaknesses. Almost all of the 24 major federal agencies had information security weaknesses in five key control categories, as illustrated in the figure below.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2009



Source: GAO analysis of IG, agency, and GAO reports.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required by FISMA. As a result, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Opportunities exist to enhance federal cybersecurity through a concerted response to safeguarding systems that include several components. First, agencies can implement the hundreds of recommendations GAO and inspectors general have made to resolve control deficiencies and information security program shortfalls. In addition, OMB's continued efforts to improve reporting and oversight as recommended by GAO could help assess agency programs. Finally, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.