October 2011

INFORMATION SECURITY

Weaknesses Continue Amid New Federal Efforts to Implement Requirements

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-137, a report to congressional committees

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security can lead to serious consequences—such as intrusions by malicious individuals, compromised networks, and the theft of sensitive information including personally identifiable information—and has identified information security as a governmentwide high-risk area. The Federal Information Security Management Act of 2002 (FISMA) established information security program, evaluation, and annual reporting requirements for federal agencies. The act requires the Office of Management and Budget (OMB) to oversee and report to Congress on agency information security policies and practices, including agencies' compliance with FISMA.

FISMA also requires that GAO periodically report to Congress on (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) agencies' implementation of FISMA requirements. To do this, GAO analyzed information security-related reports and data from 24 major federal agencies, their inspectors general, OMB, and GAO.

What GAO Recommends

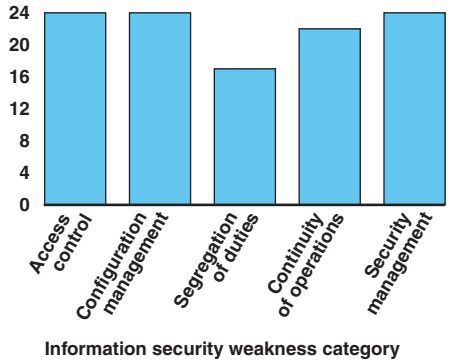
GAO is recommending that the Director of OMB provide performance targets for metrics included in OMB's annual FISMA reporting instructions to agencies and inspectors general. OMB stated it was more appropriate for those targets to be included in the performance metrics that are now issued separately by the Department of Homeland Security. GAO agrees that this meets the intent of its recommendation.

View GAO-12-137. For more information, contact Gregory C.Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Weaknesses in information security policies and practices at 24 major federal agencies continue to place the confidentiality, integrity, and availability of sensitive information and information systems at risk. Consistent with this risk, reports of security incidents from federal agencies are on the rise, increasing over 650 percent over the past 5 years. Each of the 24 agencies reviewed had weaknesses in information security controls (see figure). An underlying reason for these weaknesses is that agencies have not fully implemented their information security programs. As a result, they have limited assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise. In reports for fiscal years 2010 and 2011, GAO and agency inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve control deficiencies and information security program shortfalls. Agencies generally agreed with most of GAO's recommendations and indicated that they would implement them.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2010



Source: GAO analysis of agency, inspectors general, and GAO reports.

OMB, agencies, and the National Institute of Standards and Technology took actions intended to improve the implementation of security requirements, but more work is necessary. Beginning in fiscal year 2009, OMB provided agencies with a new online tool to report their information security postures and, in fiscal year 2010, instituted the use of new and revised metrics. Nevertheless, OMB's guidance for those metrics did not always provide performance targets for measuring improvement. In addition, weaknesses were identified in the processes agencies used to implement requirements. Specifically, agencies did not always ensure (1) personnel with significant responsibilities received training; (2) security controls were monitored continuously; (3) weaknesses were remediated effectively; and (4) incidents were resolved in a timely manner, among other areas. Until hundreds of recommendations are implemented and program weaknesses are corrected, agencies will continue to face challenges in securing their information and information systems.