GAO Highlights

Highlights of GAO-15-714, a report to congressional committees

September 2015

FEDERAL INFORMATION SECURITY

Agencies Need to Correct Weaknesses and Fully Implement Security Programs

Why GAO Did This Study

Since 1997, GAO has designated federal information security as a government-wide high risk area, and in 2003 expanded this area to include computerized systems supporting the nation’s critical infrastructure. In February 2015, in its high risk update, GAO further expanded this area to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

FISMA required federal agencies to develop, document, and implement an agency-wide information security program. The act also assigned OMB with overseeing agencies’ implementation of security requirements.

FISMA also included a provision for GAO to periodically report to Congress on (1) the adequacy and effectiveness of agencies’ information security policies and practices and (2) agencies’ implementation of FISMA requirements. GAO analyzed information security-related reports and data from 24 federal agencies, their inspectors general, and OMB; reviewed prior GAO work; examined documents from OMB and DHS; and spoke to agency officials.

What GAO Recommends

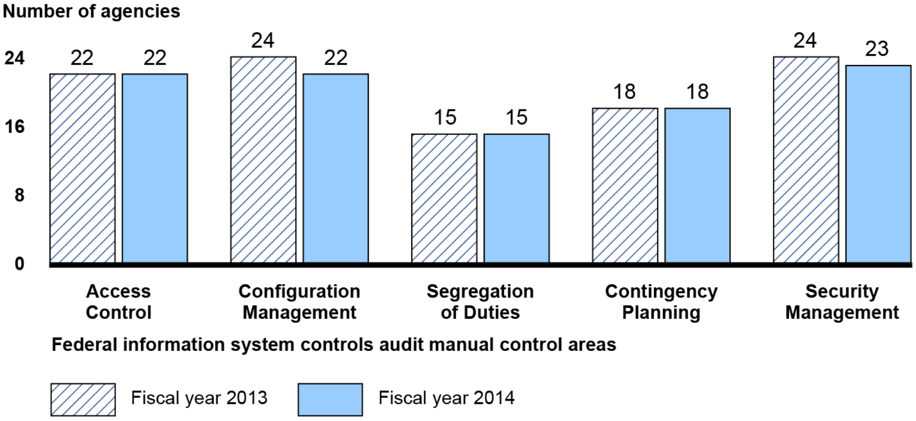
GAO is recommending that OMB, in consultation with DHS and others, enhance security program reporting guidance to inspectors general so that the ratings of agency security performance will be consistent and comparable. OMB generally concurred with our recommendation.

View GAO-15-714. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Persistent weaknesses at 24 federal agencies illustrate the challenges they face in effectively applying information security policies and practices. Most agencies continue to have weaknesses in (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis (see fig.). These deficiencies place critical information and information systems used to support the operations, assets, and personnel of federal agencies at risk, and can impair agencies’ efforts to fully implement effective information security programs. In prior reports, GAO and inspectors general have made hundreds of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented.

Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

Federal agencies’ implementation in fiscal years 2013 and 2014 of requirements set by the *Federal Information Security Management Act of 2002* (FISMA) was mixed. For example, most agencies had developed and documented policies and procedures for managing risk, providing security training, and taking remedial actions, among other things. However, each agency’s inspector general reported weaknesses in the processes used to implement FISMA requirements. In addition, to comply with FISMA’s annual reporting requirements, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) provide guidance to the inspectors general on conducting and reporting agency evaluations. Nevertheless, GAO found that this guidance was not always complete, leading to inconsistent application by the inspectors general. For example, because it did not include criteria for making overall assessments, inspectors general inconsistently reported agency security performance.