GAO Highlights

Highlights of GAO-17-549, a report to congressional committees

September 2017

FEDERAL INFORMATION SECURITY

Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices

Why GAO Did This Study

GAO first designated federal information security as a governmentwide high-risk area 20 years ago. First enacted in 2002, FISMA required federal agencies to develop, document, and implement information security programs and have independent evaluations of those programs and practices. As amended in 2014, FISMA assigns responsibilities to OMB, DHS, and NIST.

FISMA also includes a provision for GAO to periodically report to Congress on agencies' information security. The objectives of this review are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the extent to which agencies with governmentwide responsibilities have implemented their requirements under FISMA. GAO categorized information security-related weaknesses reported by the 24 CFO Act agencies, their IGs, and OMB according to the control areas defined in the Federal Information System Controls Audit Manual; reviewed prior GAO work; examined OMB, DHS, and NIST documents; and interviewed agency officials.

What GAO Recommends

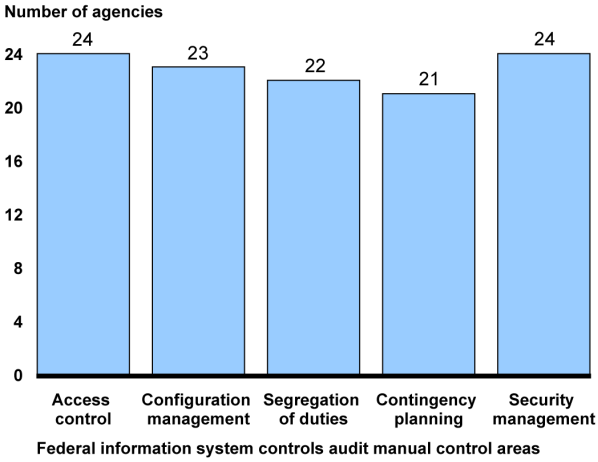
GAO recommends that OMB, in consultation with DHS and others, develop a plan and schedule to evaluate whether the full implementation of the capability maturity model developed by the Council of the Inspectors General on Integrity and Efficiency ensures that consistent and comparable results are achieved across all federal agencies. OMB generally concurred with our recommendation.

View GAO-17-549. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

During fiscal year 2016, federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices. Most of the 24 *Chief Financial Officers Act* (CFO) agencies had weaknesses in five control areas—access controls, configuration management controls, segregation of duties, contingency planning, and agencywide security management (see figure). GAO and inspectors general (IGs) evaluations of agency information security programs, including policies and practices, determined that most agencies did not have effective information security program functions in fiscal year 2016. GAO and IGs have made hundreds of recommendations to address these security control deficiencies, but many have not yet been fully implemented.

The 24 CFO Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 *Chief Financial Officers Act* agencies' information security practices and policies for fiscal year 2016. | GAO-17-549

The Office of Management and Budget (OMB), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and IGs have ongoing and planned initiatives to support implementation of the Federal Information Security Management Act of 2002 as amended by the Federal Information Security Modernization Act of 2014 (FISMA) across the federal government. OMB, in consultation with other relevant entities, has expanded the use of a maturity model developed by the Council of the Inspectors General on Integrity and Efficiency and used to evaluate additional information security performance areas each year. However, OMB and others have not developed a plan and schedule to determine whether using the security capability maturity model will provide useful results that are consistent and comparable. Until an evaluative component is incorporated into the implementation of the maturity model, OMB will not have reasonable assurance that agency information security programs have been consistently evaluated.