July 2019

FEDERAL INFORMATION SECURITY

Agencies and OMB Need to Strengthen Policies and Practices

GAO Highlights

Highlights of GAO-19-545, a report to congressional committees

Why GAO Did This Study

For 22 years, GAO has designated information security as a government-wide high-risk area. FISMA requires federal agencies to develop, document, and implement information security programs and have independent evaluations of those programs and practices. It also assigns government-wide responsibilities for information security to OMB, DHS, and NIST.

FISMA includes a provision for GAO to periodically report to Congress on agencies' implementation of the act. GAO's objectives in this report were to (1) describe the reported adequacy and effectiveness of selected federal agencies' information security policies and practices and (2) evaluate the extent to which OMB, DHS, and NIST have implemented their government-wide FISMA requirements. GAO categorized information security deficiencies as reported by 16 randomly selected agencies and their IGs according to the elements of an information security program; evaluated IG reports for 24 CFO Act agencies; examined OMB, DHS, and NIST documents; and interviewed agency officials.

What GAO Recommends

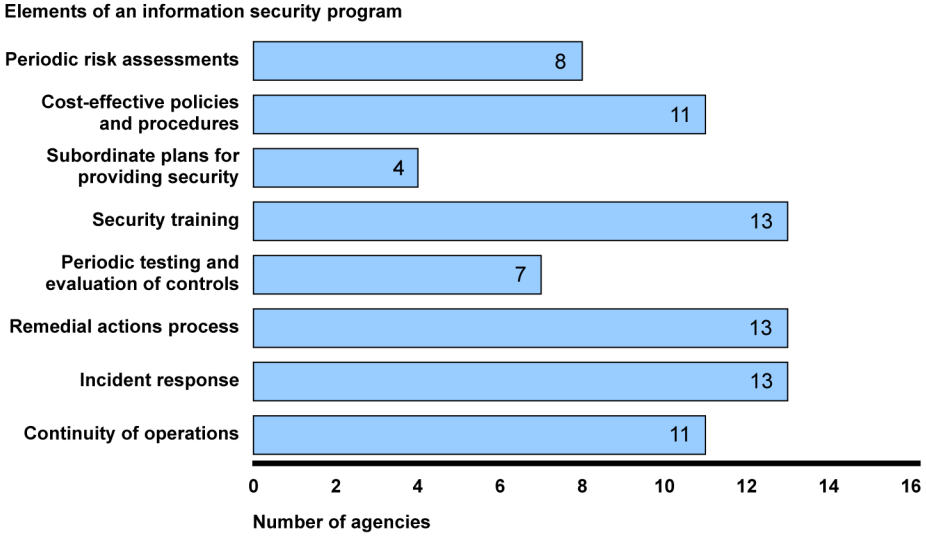
GAO is making three recommendations to OMB to (1) submit its FISMA report to Congress for fiscal year 2018, (2) expand its coordination of CyberStat meetings with agencies, and (3) collaborate with CIGIE to update the inspector general FISMA reporting metrics to include assessing system security plans. OMB generally agreed with GAO's recommendations.

View GAO-19-545. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

During fiscal year 2018, many federal agencies were often not adequately or effectively implementing their information security policies and practices. For example, most of the 16 agencies GAO selected for review had deficiencies related to implementing the eight elements of an agency-wide information security program required by the *Federal Information Security Modernization Act of 2014* (FISMA) (see figure). Further, inspectors general (IGs) reported that 18 of the 24 *Chief Financial Officers (CFO) Act of 1990* agencies did not have effective agency-wide information security programs. GAO and IGs have previously made numerous recommendations to agencies to address such deficiencies, but many of these recommendations remain unimplemented.

Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Information Security Program, as Required by the *Federal Information Security Modernization Act of 2014*



Source: GAO analysis of agency, inspector general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-19-545

With certain exceptions, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST) were generally implementing their government-wide FISMA requirements, including issuing guidance and implementing programs that are intended to improve agencies' information security. However, OMB has not submitted its required FISMA report to Congress for fiscal year 2018 and has reduced the number of agencies at which it holds CyberStat meetings from 24 in fiscal year 2016 to three in fiscal year 2018—thereby restricting key activities for overseeing agencies' implementation of information security. Also, OMB, in collaboration with the Council of Inspectors General for Integrity and Efficiency (CIGIE), did not include a metric for system security plans, one of the required information security program elements, in its guidance on FISMA reporting. As a result, oversight of agencies' information security programs was diminished.