March 2022

CYBERSECURITY

OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision

GAO Highlights

Highlights of GAO-22-104364, a report to congressional committees

Why GAO Did This Study

Since 1997, GAO has designated information security as a government-wide high-risk area. To protect federal information and systems, FISMA requires federal agencies to develop, document, and implement information security programs. Congress included a provision in FISMA for GAO to periodically report on agencies' implementation of the act.

GAO's objectives in this report were to (1) describe the reported effectiveness of federal agencies' implementation of cybersecurity policies and practices and (2) evaluate the extent to which relevant officials at federal agencies consider FISMA to be effective at improving the security of agency information systems.

To do so, GAO reviewed the 23 civilian CFO Act agencies' FISMA reports, agency reported performance data, past GAO reports, and OMB documentation and guidance. GAO also interviewed agency officials from the 24 CFO Act agencies (i.e., the 23 civilian CFO Act agencies and the Department of Defense), the Council of IGs on Integrity and Efficiency, and OMB.

What GAO Recommends

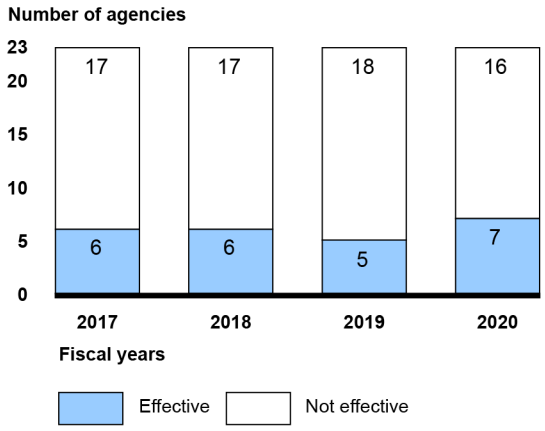
GAO is making two recommendations that OMB, in consultation with others, clarify its guidance to IGs and create a more precise overall rating scale. OMB did not concur with our recommendations, stating, in part, that they want to provide IGs with the flexibility to adapt their reviews. Nevertheless, GAO believes that the recommendations are warranted in order to provide a more consistent and accurate picture of agencies' cybersecurity performance.

View GAO-22-104364. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

What GAO Found

In fiscal year 2020, the effectiveness of federal agencies' implementation of requirements set by the *Federal Information Security Modernization Act of 2014* (FISMA) was mixed. For example, more agencies reported meeting goals for managing the security of their software assets, as well as for intrusion detection and prevention. Nevertheless, inspectors general (IG) identified agencies' uneven performance of cybersecurity practices. For fiscal year 2020, IGs determined that seven of the 23 civilian *Chief Financial Officers* (CFO) *Act of 1990* agencies had effective information security programs. Between fiscal years 2017 and 2020, the percentage of agencies receiving effective ratings has generally been consistent, ranging from 22 to 30 percent.

Number of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies with Effective and Not Effective Agency-Wide Information Security Programs, as Reported by Inspectors General for Fiscal Years 2017-2020



Source: GAO analysis of inspector general report data and Office of Management and Budget's *Federal Information Security Modernization Act of 2014* reports to Congress. | GAO-22-104364

According to officials at all 24 CFO Act agencies, FISMA and its associated reporting process enabled their agencies to improve their information security programs' effectiveness. Specifically, Chief Information Officers and Chief Information Security Officers at 14 agencies stated that FISMA improved program effectiveness to a great extent, while officials at 10 agencies said it improved effectiveness to a moderate extent.

As required under FISMA, the Office of Management and Budget (OMB), in partnership with other organizations, provides guidance to IGs on conducting and reporting agency FISMA evaluations. GAO found that this guidance was not always clear, leading to inconsistent application by IGs. Further, GAO found that OMB's overall IG rating scale of "effective" and "not effective" resulted in imprecise ratings that did not clearly distinguish the differing levels of agencies' implementation of cybersecurity requirements. As a result, IG ratings may be less useful for cybersecurity oversight. By clarifying its future ratings guidance and improving its rating scale, OMB could help ensure that the reviews provide a more consistent picture of agencies' cybersecurity performance, enabling Congress to better understand agencies' relative cybersecurity risks.