GAO Highlights

Highlights of GAO-22-105637, a testimony before the Committee on Oversight and Reform, House of Representatives

January 2022

CYBERSECURITY

Preliminary Results Show that Agencies' Implementation of FISMA Requirements Was Inconsistent

Why GAO Did This Study

Federal systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. Without proper safeguards, computer systems are increasingly vulnerable to attack. As such, since 1997, GAO has designated information security as a government-wide high-risk area.

FISMA was enacted to provide federal agencies with a comprehensive framework for ensuring the effectiveness of information security controls. FISMA requires federal agencies to develop, document, and implement an information security program to protect the information and systems that support the operations and assets. It also includes a provision for GAO to periodically report on agencies' implementation of the act.

This testimony discusses GAO's preliminary results from its draft report in which the objectives 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.

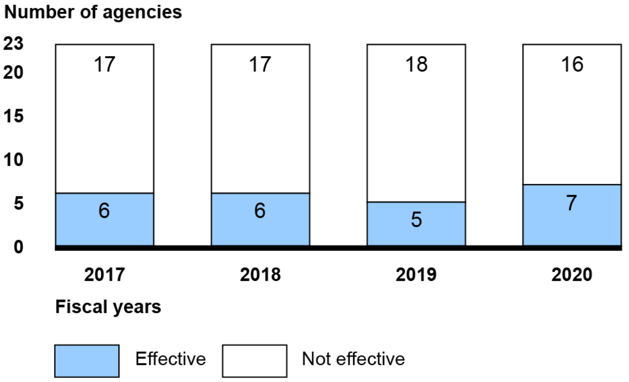
To do so, GAO reviewed the 23 civilian CFO Act agencies' FISMA reports, agency-reported performance data, past GAO reports, and OMB documentation and guidance. GAO also interviewed agency officials from the 24 CFO Act agencies (i.e., the 23 civilian CFO Act agencies and the Department of Defense).

View GAO-22-105637. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Based on GAO's preliminary results, in fiscal year 2020, the effectiveness of federal agencies' implementation of requirements set by the *Federal Information Security Modernization Act of 2014* (FISMA) varied. For example, more agencies reported meeting goals related to capabilities for the detection and prevention of cybersecurity incidents, as well as those related to access management for users. However, inspectors general (IG) identified uneven implementation of cyber security policies and practices. For fiscal year 2020 reporting, IGs determined that seven of the 23 civilian *Chief Financial Officers Act of 1990* (CFO) agencies had effective agency-wide information security programs. The results from the IG reports for fiscal year 2017 to fiscal year 2020 were similar with a slight increase in effective programs for 2020.

Number of 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-22-105637

GAO has also routinely reported on agencies' inconsistent implementation of federal cybersecurity policies and practices. Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings; about 900 were not yet fully implemented as of November 2021. More recent GAO reviews have identified weaknesses regarding access controls, configuration management, and the protection of data shared with external entities. GAO has made numerous recommendations to address these.

Based on interviews with agency officials, such as chief information security officers, GAO's preliminary results show that officials at 14 CFO Act agencies stated that FISMA enabled their agencies to improve information security program effectiveness to a great extent. Officials at the remaining 10 CFO Act agencies said that FISMA had improved their programs to a moderate extent. The officials also identified impediments to implementing FISMA, such as a lack of resources. Agency officials suggested ways to improve the FISMA reporting process, such as by updating FISMA metrics to increase their effectiveness, improving the IG evaluation and rating process, and increasing the use of automation in report data collection.