GAO Highlights

Highlights of GAO-24-106291, a report to congressional committees

January 2024

CYBERSECURITY

OMB Should Improve Information Security Performance Metrics

Why GAO Did This Study

To protect federal information and systems, FISMA requires federal agencies to develop, document, and implement information security programs. FISMA includes a provision for GAO to periodically report on agencies' implementation of the act.

GAO's objectives in this report were to identify (1) the reported effectiveness of agencies' efforts to implement FISMA; (2) the key practices used by agencies to meet FISMA requirements; and (3) how FISMA metrics could be changed to better measure the effectiveness of federal agency information security programs.

To do so, GAO reviewed the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies' FISMA reports, agency reported performance data, and OMB documentation and guidance. The Department of Defense (DOD) was not included in GAO's analysis of performance data due to DOD's classification of the information. GAO also solicited perspectives from the 24 CFO Act agencies (including DOD) and interviewed officials with the Council of Inspectors General on Integrity and Efficiency, the Cybersecurity and Infrastructure Security Agency, and OMB.

What GAO Recommends

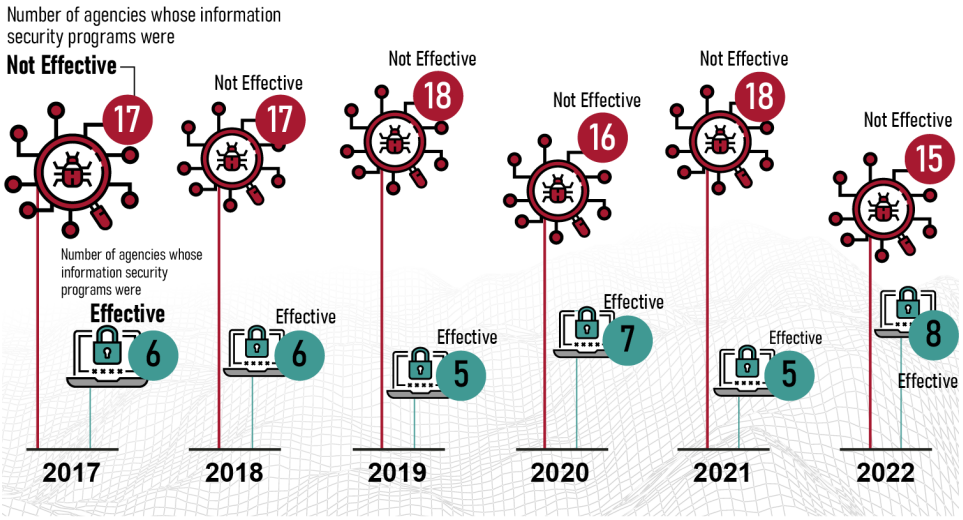
GAO is making two recommendations for OMB to collaborate with its partners to enhance FISMA metrics that can lead to more effective programs and performance. OMB neither agreed nor disagreed with the recommendations and provided technical comments that were incorporated as appropriate.

View GAO-24-106291. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

What GAO Found

Federal agencies' implementation of the Federal Information Security Modernization Act of 2014 (FISMA) continued to be mostly ineffective. Although some improvement was reported from 2021 to 2022, inspectors general (IG) of 15 of the 23 civilian agencies found the information security programs to be ineffective (see figure). IGs reported various causes for the ineffective programs, including management accountability issues and gaps in standards and quality control. Addressing the causes could improve the federal government's cybersecurity posture.

23 Chief Financial Officers Act of 1990 Agencies That Do or Do Not Have Effective Information Security Programs, as Reported by Inspectors General, Fiscal Years 2017 through 2022.



Sources: GAO (analysis); civilian agencies subject to Chief Financial Officers Act of 1990 (data); PST Vector/stock.adobe.com (background); lovemask/stock.adobe.com (icons). | GAO-24-106291

Agency officials identified various practices that have contributed to improving the effectiveness of their agency's information security program. Specifically, officials most often highlighted internal communication; organizational characteristics, such as leadership commitment; and centralized policies and procedures as being essential to effectively implement FISMA.

The Office of Management and Budget (OMB), in collaboration with other oversight groups, provides metrics to evaluate the effectiveness of federal information security programs and implementation of FISMA. However, agencies and IGs stated that some FISMA metrics are not useful because they do not always accurately evaluate information security programs. Agencies and IGs reported that metrics should be clearly tied to performance goals, account for workforce issues and agency size, and incorporate risk. Further, crafting metrics that address the key causes of ineffective programs could enhance their effectiveness. By modifying FISMA metrics in these ways, OMB could help ensure that the measures provide an accurate picture of agencies' information security performance.