GAO

Highlights

Highlights of GAO-25-107470, a report to congressional committees

June 2025

CYBERSECURITY

Network Monitoring Program Needs Further Guidance and Actions

Why GAO Did This Study

A key aspect of a rigorous cybersecurity program is continuously monitoring networks and systems to identify and manage risks. Consistent with the FISMA requirement for agency network monitoring, the CISA-led CDM program provides tools to agencies to assist in this effort.

FISMA includes a provision for GAO to periodically report on agencies' implementation of the act. Among its objectives, this report examines the extent to which the CDM program is (1) meeting its goals, and (2) supporting other federal cybersecurity initiatives.

GAO selected for review the 23 civilian agencies covered in the Chief Financial Officers Act of 1990 (CFO Act). GAO compared CDM program documentation against relevant guidance, and summarized survey results from the 23 civilian CFO Act agencies. GAO also interviewed CISA and OMB officials.

What GAO Recommends

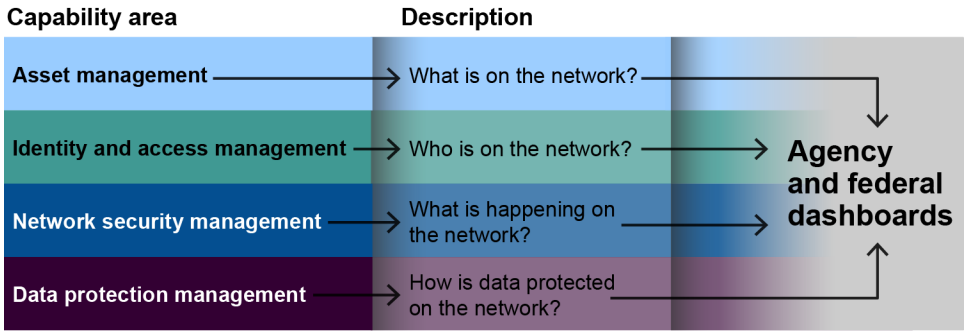
GAO is making four recommendations to DHS and CISA to (1) issue guidance on implementing network security and data protection capabilities, (2) address data quality issues, (3) implement an endpoint solution, and (4) issue updated guidance on cloud asset management. DHS, on behalf of CISA, concurred with the recommendations.

For more information, contact Jennifer R. Franks at franksj@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) program in 2012 to strengthen the cybersecurity of government networks and systems. Its goals are to: (1) reduce exposure to insecure configurations or known vulnerabilities; (2) improve federal cybersecurity response capabilities; (3) increase visibility into the federal cybersecurity posture; and (4) streamline Federal Information Security Modernization Act of 2014 (FISMA) reporting. The Cybersecurity and Infrastructure Security Agency (CISA) manages these goals across four capability areas (see figure). The program is meeting two of its four goals and partially meeting the other two, as discussed below.

Figure: Continuous Diagnostics and Mitigation Capability Areas



Source: GAO analysis of Department of Homeland Security data. | GAO-25-107470

CDM has met two goals. First, it is reducing exposure to insecure configurations and known vulnerabilities—22 of 23 agencies reported that the program was helpful in accomplishing this. CDM is also meeting its incident response capability goal.

The program, however, has been less successful in meeting the other two goals.

- Although CISA developed dashboards to visualize and provide insight to the federal cybersecurity posture and the associated capability areas noted above, officials from 21 of 23 agencies stated that they had not yet fully implemented network security and data protection capabilities. Several agencies cited a lack of guidance as contributing to the slow implementation.
- While officials from four agencies stated that CDM helped to automate FISMA reporting, officials from seven other agencies said that data quality issues were adversely affecting efforts to streamline reporting leading to manual updates to correct data errors.

Regarding supporting other initiatives, the Office of Management and Budget (OMB) established expectations that CDM would support federal cybersecurity efforts on zero trust architecture, endpoint detection and response, and cloud asset management. CDM has generally met expectations for the zero trust architecture program. However, CISA had not finalized key activities to support endpoint detection and cloud asset management. CISA's actions to implement an endpoint solution for all agencies and issue updated guidance on cloud asset management would improve the cybersecurity posture of federal agencies.