GAO Highlights

Highlights of GAO-24-105658, a report to the Chairman of the Committee on Homeland Security and Governmental Affairs, U.S. Senate

December 2023

CYBERSECURITY

Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements

Why GAO Did This Study

Cyber-based attacks on federal systems have become more damaging and disruptive. The Federal Information Security Modernization Act of 2014 (FISMA) requires that agency information security programs include procedures for detecting, reporting, and responding to security incidents. Executive Order (EO) 14028 builds on FISMA and establishes priorities for the federal executive branch to improve efforts to protect against and respond to persistent and malicious cyber campaigns. The EO and OMB and CISA guidance require agencies to address these priorities.

GAO's objectives were to (1) describe the capabilities agencies use to prepare for and respond to cybersecurity incidents, (2) evaluate the extent to which agencies have made progress in preparing for cybersecurity incident response, and (3) describe the challenges agencies face in preparing for incident response and the efforts to address them.

GAO interviewed officials and reviewed documentation from the 24 CFO Act agencies, CISA, and OMB on their capabilities, progress, and challenges in cybersecurity incident response. GAO analyzed questionnaire responses to evaluate agencies' progress in incident response preparation. The Department of Defense was excluded from some analysis because it was not subject to all requirements.

What GAO Recommends

GAO is making 20 recommendations to 19 agencies to, among other things, fully implement event logging requirements. Sixteen agencies agreed with the recommendations and three neither agreed nor disagreed.

View GAO-24-105658. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Federal agencies rely upon the following for cybersecurity incident response:

- tools, such as endpoint detection and response solutions;
- services, such as threat hunting or cyber threat intelligence provided by the Cybersecurity and Infrastructure Security Agency (CISA) and third party firms; and
- resources, such as skilled staff and funding.

The 23 civilian Chief Financial Officers (CFO) Act of 1990 agencies have made progress in cybersecurity incident response preparedness by taking steps to standardize their incident response plans and demonstrating improvement in their capabilities for incident detection, analysis, and handling (see table).

Executive Order 14028 Cybersecurity Incident Response Requirements and Status of Completion, as of August 2023

Requirement	Status
Agencies are to use the Cybersecurity and Infrastructure Security Agency playbook (issued in November 2021) for planning and conducting cybersecurity vulnerability and incident response activities for agency information systems	Agencies have incorporated or are incorporating the playbook into their plans, and all 23 agencies substantially completed the preparation phase activities.
Agencies are to deploy an endpoint detection and response initiative and work toward ensuring coverage on 80 percent of endpoints	All 23 agencies have begun to deploy an endpoint detection and response solution, and 16 agencies have reported 80 percent or greater coverage.
Agencies are to assess their event logging maturity against the maturity model in the Office of Management and Budget's M-21-31 memorandum, identify gaps associated with completing each of the requirements, and work toward reaching event logging tier 3 by August 2023	Twenty agencies did not reach the maturity level tier 3 by the deadline.

Source: GAO analysis of agency cybersecurity incident response information. | GAO-24-105658

However, 20 agencies have not met requirements for investigation and remediation (event logging) capabilities. The Office of Management and Budget (OMB) required agencies to reach the advanced (tier 3) level by August 2023. The tier 3 level means that logging requirements at all criticality levels are met. However, as of August 2023, three of the 23 agencies were at tier 3. Of the remaining 20, three were at the basic (tier 1) level and 17 were at the not effective (tier 0) level. Until the agencies implement all event logging requirements, the federal government's ability to fully detect, investigate, and remediate cyber threats will be constrained.

Agencies described three key challenges that hindered their abilities to fully prepare to respond to cybersecurity incidents: (1) lack of staff, (2) event logging technical challenges, and (3) limitations in cyber threat information sharing. Federal entities have ongoing efforts that can assist in addressing these challenges. These efforts include onsite cyber incident response assistance from CISA, event logging workshops and guidance, and enhancements to a cyber threat information sharing platform. In addition, there are long-term efforts planned such as implementation of the *National Workforce and Education Strategy* and a new threat intelligence platform offering from CISA, targeted to roll out its first phase to federal departments and agencies in fiscal year 2024.