United States Government Accountability Office

Report to the Chairman, 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

GAO-24-105658

December 2023

CYBERSECURITY

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

GAO Highlights

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

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.

Contents

Tables

Figures

Abbreviations

Agriculture	Department of Agriculture
AIS	Automated Indicator Sharing
CDM	continuous diagnostics and mitigation
CFO	Chief Financial Officers
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COOP	continuity of operations plan
DHS	Department of Homeland Security
DOD	Department of Defense
EDR	endpoint detection and response
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FISMA	Federal Information Security Modernization Act of 2014
HIRT	Hunt and Incident Response Team
ICOAST	Intelligence Community Analysis and Signature Tool
IG	Inspector General
IT	information technology
MOA	memoranda of agreement
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
SBA	Small Business Administration
USAID	U.S. Agency for International Development
US-CERT	United States Computer Emergency Readiness Team

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 4, 2023

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman:

Cyber-based attacks on federal systems have become more damaging and disruptive. Protecting the information systems and the information that resides on them and effectively responding to a cyber incident is important to federal agencies.[1] This is because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

Additionally, a series of high-profile cyber incidents (e.g., SolarWinds[2] and the Colonial Pipeline attacks[3]) demonstrated the need to move with urgency to take actions that would improve the security of U.S. government IT systems and strengthen the federal role in protecting critical infrastructure. Further, a May 2021 executive order marked a renewed commitment to cybersecurity and specifically prioritized incident

[1]A cyber incident is a security breach of a computerized system and information and, for the purposes of this report, has the same meaning as a computer security incident, which the National Institute of Standards and Technology defines as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The terms information security and information security incident apply more broadly to any forms of information and systems.

[2]As we previously reported, beginning in September 2019, a campaign of cyberattacks by a foreign threat actor breached the computing networks at SolarWinds—a network management software company widely used in the federal government to monitor network activity on federal systems. GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents,* GAO-22-104746 (Washington, D.C.: Jan. 13, 2022).

[3]On May 7, 2021, the Colonial Pipeline Company learned that it was the victim of a cyberattack. Malicious actors reportedly deployed “ransomware” against the pipeline company’s business systems. GAO, *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic),* (Washington, D.C.: May 18, 2021). https://www.gao.gov/blog/colonial-pipelinecyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic (accessed March 16, 2023).

response, including making the prevention, detection, assessment, and remediation of cyber incidents a top priority.[4]

Given that emphasis, you asked us to review the capabilities of federal agencies to respond to cybersecurity incidents impacting government systems. Our specific objectives were to (1) describe the capabilities federal agencies rely upon to prepare for and respond to cybersecurity incidents; (2) evaluate the extent to which federal agencies have made progress in preparing for cybersecurity incident response activities since the issuance of Executive Order 14028; and (3) describe the challenges federal agencies face in preparing for cybersecurity incident response and what federal efforts, if any, can assist agencies with these challenges.

To address the first objective, we reviewed documentation from the 24 Chief Financial Officers (CFO) Act of 1990 agencies, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST) to identify the range of cybersecurity incident response tools and services agencies have in place.[5] Such documentation included federal incident response guidance, agencies' incident response staffing plans, and budget requests and funding sources for cybersecurity incident response enhancements. Furthermore, we interviewed officials from the 24 CFO Act agencies, CISA, and OMB.

To address the second objective, we identified key requirements within Executive Order 14028, associated Office of Management and Budget (OMB) memoranda, and a CISA Binding Operational Directive. These requirements dictate that federal agencies are to make improvements to federal cybersecurity incident response standardization; detection and

[4]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[5]The CFO Act of 1990 established a CFO position at major federal agencies, referred to as CFO Act agencies. There are 24 agencies identified in the CFO Act: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

remediation efforts, such as endpoint detection and response (EDR);[6] continuous diagnostics and mitigation (CDM);[7] and augmented event logging.[8] We reviewed and analyzed documentation from the 23 civilian agencies and CISA to assess their progress in meeting key requirements.[9] We also interviewed relevant agency officials.

To address the third objective, we interviewed officials from all 24 CFO Act agencies and CISA. We requested information and documentation regarding challenges agencies have experienced with cybersecurity incident response. We also requested information regarding any challenges agencies have had in meeting executive branch requirements; receiving incident response assistance; and collecting, aggregating, and sharing cyber threat intelligence data.

We also requested information and documentation on what federal efforts could assist with the challenges. Through our interviews and data collection efforts, we categorized and grouped incident response preparation challenges. We also categorized and grouped assistance efforts that could help overcome the challenges agencies identified. For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from January 2022 to December 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]OMB, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,* M-22-01 (Washington, D.C.: Oct. 8, 2021).

[7]OMB*, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* M-22-05 (Washington, D.C.: Dec. 6, 2021); and *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements,* M-23-03 (Dec. 2, 2022, rescinded M-22-05).

[8]OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: Aug. 27, 2021).

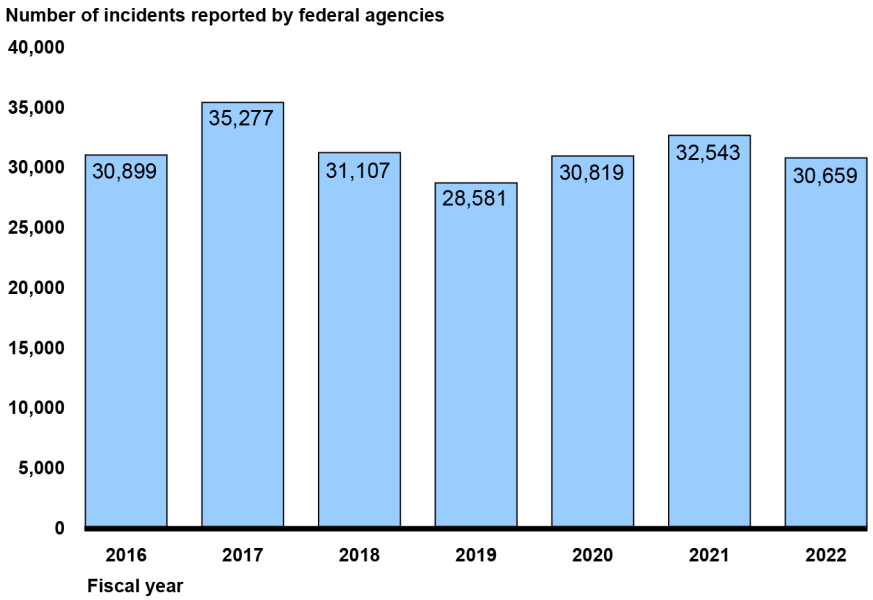
[9]We excluded the Department of Defense from our analysis as it was not subject to the OMB and CISA requirements used in our review.

Background

IT systems supporting federal agencies are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising federal systems and networks. Compounding these risks, federal systems and networks are often interconnected with other internal and external systems and networks, including the internet, thereby increasing the number of avenues of attack and expanding their potential attack surface.

The emergence of increasingly sophisticated threats and the frequency of cyber incidents underscores the continuing and urgent need for effective information security. Threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. The number of information security incidents reported by federal agencies to DHS's United States Computer Emergency Readiness Team (US-CERT) was 30,659 incidents in fiscal year 2022, as reflected in figure 1.

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2016 through 2022



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data. | GAO-24-105658

For fiscal year 2022, OMB reported three major incidents, all involving personally identifiable information, at the Departments of Agriculture, Education, and the Treasury. In addition, there have already been numerous cyber incidents reported at federal agencies this year.[10] For example, in February 2023, the U.S. Marshal Service experienced a ransomware attack that affected a network containing sensitive law enforcement information.[11] In the same month, the Consumer Financial Protection Bureau became aware of an incident. This incident involved an employee who made an unauthorized transfer of records containing personal information on approximately 256,000 consumers at one institution, as well as confidential supervisory information at 45 institutions.[12]

Further, in May 2023, the Department of Transportation suffered a data breach on administrative systems potentially exposing the personal information of approximately 237,000 current and former agency employees, according to media reports.[13] The systems are used to process employee transit benefits; however, the breach did not affect any transportation safety systems, according to the article.

Finally, in June 2023, the Federal Bureau of Investigation (FBI) and CISA released a joint cybersecurity advisory stating that beginning in May 2023 a malicious actor began exploiting a vulnerability in a managed file transfer software solution, MOVEit. This software was used by multiple organizations, including federal agencies, and the exploitation resulted in the theft of sensitive data.[14]

These examples highlight the federal government's need to be fully prepared to respond to, manage, mitigate, and learn from cybersecurity incidents. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their

[10]OMB, *Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2022* (Washington, D.C.: May 1, 2023).

[11]https://www.nbcnews.com/politics/politics-news/major-us-marshals-service-hack-compromises-sensitive-info-rcna72581.

[12]https://www.wsj.com/articles/in-major-incident-cfpb-says-staffer-sent-250-000-consumers-data-to-personal-account-fdc0a540.

[13]https://www.nextgov.com/cybersecurity/2023/05/hack-transportation-systems-exposes-employee-information/386364/.

[14]FBI and CISA Joint Cybersecurity Advisory, AA23-158A *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability* (June 7, 2023).

access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

Federal Law and Guidance Have Been Established to Improve Cyber Incident Response

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their operations and assets.[15] FISMA requires that agency information security programs include procedures for detecting, reporting, and responding to security incidents and that agencies report annually on the total number of information security incidents to OMB and Congress.

FISMA also requires agencies to comply with OMB's policies and procedures, DHS's binding operational directives, and NIST's federal information standards and guidelines. NIST has responsibility for developing standards and guidelines, including minimum requirements, for securing the information systems used or operated by a federal agency, contractor of an agency, or other organization on behalf of an agency. NIST has issued special publications that guide agencies, including those for detecting and handling cyber incidents. Specifically, NIST Special Publication 800-61 provides guidance on policies, plans, and procedures for implementing incident response.[16] The publication has guidelines for establishing an effective incident response program, including detecting, analyzing, prioritizing, reporting, and handling an incident.

The Cybersecurity Information Sharing Act of 2015 created a framework to facilitate and promote the voluntary sharing of cyber threat indicators and defensive measures among and between federal and non-federal entities. Under the act, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of appropriate federal entities, are to jointly develop and issue procedures to facilitate and promote the timely sharing of classified cyber threat indicators and defensive

[15]44 U.S.C. § 3554(b).

[16]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication (SP) 800-61, Revision 2 (Gaithersburg, MD: August 2012).

measures.[17] In addition, the Inspectors General (IG) of the appropriate federal entities in consultation with the IG of the Intelligence Community and the Council of Inspectors General on Financial Oversight are to jointly report to Congress every 2 years regarding the actions taken to carry out the act.[18]

The act, among other things, called for the establishment of a cyber threat information sharing capability and process. In response, in 2016, DHS developed and implemented the Automated Indicator Sharing platform (AIS), a service that enables the real-time exchange of machine-readable cyber threat indicators and defensive measures between public and private sector organizations. AIS helps to protect the participants of the service and ultimately reduce the prevalence of cyberattacks. Then, in 2017, the Office of the Director of National Intelligence (ODNI) developed and deployed the Intelligence Community Analysis and Signature Tool (ICOAST) to expand accessibility and sharing of cyber threat indicators and defensive measures with the intelligence community.

Issued by the President in 2021, Executive Order 14028 focuses on the nation's cybersecurity by requiring various security controls to be implemented across federal agencies.[19] Specifically, the executive order states that the federal government must improve its efforts to identify, deter, protect against, detect, and respond to persistent and increasingly sophisticated malicious cyber campaigns. Further, it states that the federal government must also carefully examine what occurred during any major cyber incident and apply lessons learned. The major goals set out by the order are for agencies to:

[17]Pub. L. No. 114-113, div. N, §§ 102(3), 103, 129 Stat. 2935, 2939 (2015). Appropriate federal entities include the Department of Commerce, the Department of Defense, the Department of Energy, DHS, the Department of Justice, the Department of the Treasury, and ODNI.

[18]See, e.g., Office of the Inspector General of the Intelligence Community, Unclassified *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2021-002 (Washington, D.C.: Dec. 9, 2021); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2019-005-U (Washington, D.C.: Dec. 19, 2019); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2017-005-U (Washington, D.C.: Dec. 19, 2017).

[19]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

- implement a standard set of operational procedures for responding to cybersecurity vulnerabilities and incidents (called the federal playbook),
- improve detection of vulnerabilities and incidents on federal networks, and
- improve federal investigative and remediation capabilities (event logging).

The executive order set forth initial requirements for agencies, CISA, OMB, and others to take specific actions or develop further recommendations or guidance. Table 1 describes the executive order's cybersecurity incident response priorities and the initial and subsequent requirements issued to achieve those goals.

Table 1: Executive Order 14028 Cybersecurity Incident Response Priorities and Related Requirements

Priorities	Source and title	Summary of requirements
Standardize the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028, May 12, 2021	• Cybersecurity and Infrastructure Security Agency (CISA) is to develop a standard set of operational procedures (playbook) to be used by agencies in planning and conducting a cybersecurity vulnerability and incident response activity. • Federal agencies are to use the CISA playbook (issued in November 2021), including any updates, for planning and conducting cybersecurity vulnerability and incident response activities for agency information systems.
Improve the Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks	The White House, Executive Order 14028	• Agencies are to establish or update memoranda of agreement (MOA) with CISA for the continuous diagnostics and mitigation (CDM) program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law. • Agencies are to deploy an endpoint detection and response (EDR) initiative to support proactive detection of cybersecurity incidents within federal government infrastructure, active cyber hunting, and containment and remediation.
	Office of Management and Budget, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01), October 8, 2021	• Federal agencies are to conduct an analysis, in coordination with CISA, to assess the current status of their EDR capabilities by identifying any gaps in existing EDR deployments. • CISA is to take four actions: develop (1) a process for continuous performance monitoring, (2) recommendations on ways to further accelerate government-wide EDR efforts, (3) a technical reference architecture and maturity model for agency consumption, and (4) a playbook of best practices for EDR solution deployments.

Priorities	Source and title	Summary of requirements
	Office of Management and Budget, Fiscal Year 2021-2022 *Guidance on Federal Information Security and Privacy Management Requirements* (M-22-05), December 6, 2021 (rescinded by M-23-03, Dec. 2, 2022)	• CISA was required to perform a program review of CDM and incorporate lessons learned into a strategy to continue improving the program for fiscal year 2022. • CISA, in coordination with the Office of Management and Budget and National Institute of Standards and Technology, was required to develop a strategy to continue to evolve machine-readable data standards for cybersecurity performance and compliance data through CDM (or a successor process).
	Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Binding Operational Directive 23-01: *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, October 3, 2022	• By April 3, 2023, agencies and CISA, through the CDM program, are to deploy an updated CDM Dashboard configuration that enables access to object-level vulnerability enumeration data for CISA analysts, as authorized in the executive order on *Improving the Nation's Cybersecurity*.
	Office of Management and Budget, Fiscal Year 2023 *Guidance on Federal Information Security and Privacy Management Requirements* (M-23-03), December 2, 2022	• Federal agencies are to report at least 80 percent of government-furnished equipment through the CDM program by the end of fiscal year 2023. • By January 2023, CISA is to begin providing OMB monthly data on CDM implementation progress by all federal agencies.
Improve the Federal Government's Investigative and Remediation Capabilities	The White House, Executive Order 14028	• OMB is to formulate policies for agencies to establish requirements for logging, log retention, and log management.
	Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31), August 27, 2021	• Federal agencies are to assess their event logging maturity against the maturity model in the memorandum, identify gaps associated with completing each of the requirements, and work toward reaching maturity levels within established time frames.

Source: GAO analysis of federal executive branch requirements. | GAO-24-105658

GAO Has Previously Reported on Agencies' Cybersecurity Incident Response

We first designated information security as a government-wide high-risk area in 1997. Since then, we have frequently reported on federal agencies' cybersecurity incident response programs. For example, in 2014, we reported that 24 major federal agencies did not consistently demonstrate that they were effectively responding to cyber incidents.[20] Specifically, we found that although all six selected agencies that we reviewed in-depth had developed parts of policies, plans, and procedures to guide their incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. We recommended that OMB and DHS better guide agencies' incident

[20]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

response procedures and we made 28 recommendations to all six selected agencies to strengthen their incident response preparation. Agencies generally concurred with and subsequently implemented all 28 recommendations.

In 2016, we reported that the Food and Drug Administration (FDA) did not fully implement elements of its incident response program.[21] We made 15 recommendations to FDA to fully implement its agency-wide information security program, including that it review and update information security procedures and policies. The agency concurred with our recommendations and has implemented all 15.

In 2020, we reported that selected agencies had generally deployed tools to continuously monitor their networks to support DHS's CDM program. However, they had not effectively implemented all key CDM program requirements.[22] We recommended that the selected agencies implement the key requirements while also recommending that DHS ensure the agency practices aligned with CDM requirements. Although the agencies and DHS concurred with the recommendations, four of the nine agency recommendations remain open and one of the six DHS recommendations is not yet implemented.

In November 2022, we reported that the Department of Defense (DOD) had not fully implemented its practices for managing cyber incidents. For example, we reported that the department had published guidance assigning overall responsibilities for protecting the DOD network against unauthorized activity or cyber threats, but the department could not always demonstrate that it had notified appropriate leadership of relevant critical incidents.[23] At the time, we recommended that DOD assign responsibility for overseeing cyber incident reporting and leadership notification and ensuring policy compliance. DOD concurred with our recommendation. To address this recommendation, in November 2023 officials reported that the department's Chief Information Officer completed a document intended to clarify the policy, responsibilities, and

[21]GAO, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk*, GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

[22]GAO, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020).

[23]GAO, *DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared*, GAO-23-105084 (Washington, D.C.: Nov.14, 2022).

procedures for cyber incident response. We will determine the status of this recommendation after fully evaluating the document.

In January and February 2023, we released a series of four reports that lay out the main cybersecurity areas the federal government should urgently address, including securing federal systems and information.[24] We summarized previous reports' key recommendations, including those to enhance the federal response to cyber incidents to better protect federal systems and information.

Agencies Rely Upon Tools, Services, and Resources for Incident Response

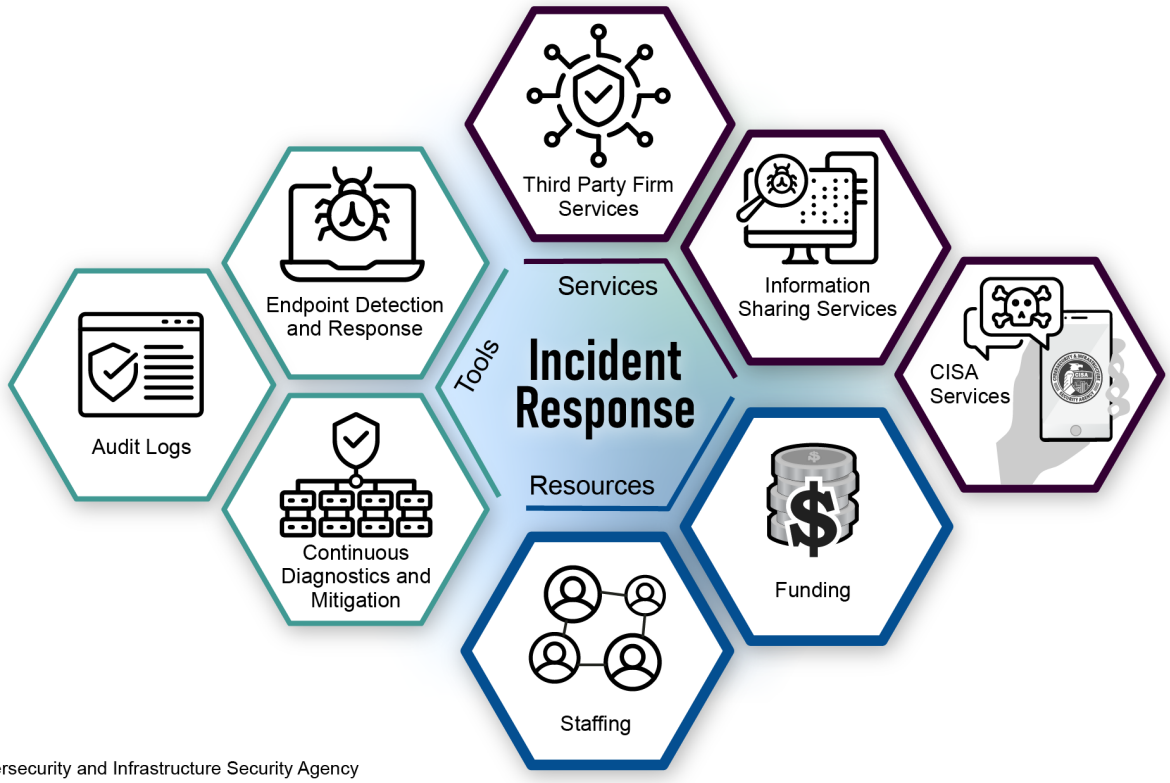
Agencies rely upon tools, services, and resources for cybersecurity incident response. Specifically, they depend on:

- tools, such as endpoint detection and response (EDR) solutions and the Continuous Diagnostics and Mitigation (CDM) program;
- services, such as threat hunting or cyber threat intelligence provided by CISA and third party firms; and
- resources, such as skilled staff and funding.

Figure 2 depicts some of the tools, resources, and services that federal agencies rely upon for cybersecurity incident response.

[24]GAO, *Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information*, GAO-23-106428 (Washington, D.C.: Jan. 31, 2023).

Figure 2: Examples of Tools, Services, and Resources Federal Agencies Use for Cybersecurity Incident Response



CISA = Cybersecurity and Infrastructure Security Agency

Sources: GAO (hand/phone, money); Gofficon/stock.adobe.com (icons). | GAO-24-105658

Tools Assist Agencies in Collecting Evidence

A range of tools exist to support federal agencies incident response detection and monitoring efforts. See table 2 for a list of available tools that support incident response.

Table 2: Description of Tools That Support Cybersecurity Incident Response

Tool	Description
Anti-virus and malware detection	Provides the ability to identify and report on the presence of viruses, trojan horses, spyware, or other malicious code on or destined for a target system. Organizations typically employ malware detection mechanisms at information system entry and exit points (e.g., firewalls, email servers, web servers, proxy servers, and remote access servers) and at endpoint devices (e.g., workstations, servers, and mobile computing devices) on the network to detect and remove malicious code transported by email, email attachments, web accesses, removable media or other means, or inserted through the exploitation of information system vulnerabilities.

Tool	Description
Endpoint detection and response	Combines real-time continuous monitoring and collection of endpoint data (e.g., certain devices connected to agency networks such as workstations, mobile phones, and servers) with rule-based, automated response and analysis capabilities.
Data loss prevention capability	Protects the confidentiality, integrity, and availability of the data by managing the location and transfer of information across systems, network devices, databases, and other assets within an organization.
Intrusion detection and prevention system	Identifies possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators for further analysis and action.
Audit log	Records system activities chronologically, including system access and operations performed in a given period. An audit record is an individual entry in an audit log related to an audited event. Audit records from audit logs can be compiled and correlated to create an audit trail. Audit trails can assist in detecting security violations, performance problems, and flaws in applications. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.
Network flow	Logs a particular communication session occurring between networked systems. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts.
Packet sniffer	Monitors network traffic on wired or wireless networks and captures packets. The inspection of these captured packets allows IT teams to forensically analyze network traffic for investigative purposes or identify unusual activity that may affect daily network operations.
Security information and event management system	Collects raw data from one or more security controls or other direct data gathering technologies and correlates, analyzes, and represents the raw data in a way that provides a more meaningful perspective on the effectiveness of security control implementation across part or all of an organization than would data from any single technology.

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

In addition to the individual tools listed, the CDM program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures by delivering better visibility and awareness of their networks and defending against cyber adversaries. The program is intended to reduce threats and improve federal cybersecurity response through four capability areas:

- asset management,
- identity and access management,
- network security management, and
- data protection management.

Under the CDM program, DHS centrally oversees the procurement and installation of diagnostic sensors and dashboards deployed to each participating agency. Agency-level dashboards provide situational awareness to agency officials, enabling them to quickly identify which network problems to fix and empower technical managers to prioritize and

mitigate risks on their respective networks. The respective agency dashboards report summary data to a federal dashboard, managed by CISA, and are intended to provide a comprehensive summary for situational awareness across the federal government.

Services Assist Agencies in Their Response Efforts

Agencies rely upon services from CISA and third party firms to assist in cybersecurity incident response and upon services to share cybersecurity threat intelligence information.

- **CISA services**. CISA offers numerous services that can assist federal agencies with their incident response preparation, coordination, and remediation efforts. According to the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*,[25] to request assistance from CISA for potentially major incidents, agencies are to activate the federal network authorization.[26]

  Based on availability of resources and priority of incident, CISA may provide a threat hunting team, or bring in other expert agencies or third party incident response services to assist the requesting agency. For example, the Hunt and Incident Response Team (HIRT) may work with an agency to identify and contain adversary activity by finding the root cause of an incident and removing it from the agency's network.

  In addition, CISA's EINSTEIN assists agencies in detection and monitoring, and serves two key roles in federal civilian executive branch cybersecurity. First, EINSTEIN detects and blocks cyberattacks from compromising the networks of participating federal agencies. Second, it provides CISA with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself. CISA

[25]Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* (November 2021).

[26]The federal network authorization defines the terms by which DHS, US-CERT, and the associated partner agency's incident response personnel are authorized to assist an agency in searching for evidence of and mitigating a potential or confirmed intrusion into an agency's network. Incident response personnel may, among other things defined in the federal network authorization, connect to government owned or controlled devices; scan a network to search for indicators of compromise, malware, and exfiltration, and identify systems, services, settings and configurations, and possible vulnerabilities; collect forensic artifacts and search for compromise, malware, and exfiltration; and capture network traffic through EINSTEIN or CDM. The authorization is a voluntary agreement that outlines roles and responsibilities, legal and technical requirements, limits, and agency authorization for CISA to conduct certain operations once the agency activates the federal network authorization.

officials reported in May 2022 that although EINSTEIN has proven effective in detecting and preventing known threats, CISA is now modernizing the program to account for changes in the threat and technology landscape and to support the increasing adoption of cloud services and other emerging technologies.

- **Third party firm services**. Third party cybersecurity firms also provide incident response services to agencies. These services may include after hours support and cyber event investigation, threat hunting, and network defense, among others.
- **Information sharing services**. Federal agencies also rely upon services to share cybersecurity threat intelligence information. For example, AIS and ICOAST are two federal government platforms through which such data is shared. In addition, CISA also established the Shared Cybersecurity Services portfolio to share cybersecurity threat intelligence and related services to federal civilian agencies and other organizations. Specifically,
  - **AIS**. Agencies and other non-federal entities use this platform for non-classified information. According to CISA, AIS enables the timely exchange of cybersecurity threat indicators and defensive measures through machine-to-machine sharing among the private sector; federal, state, local, tribal, and territorial governments; and information sharing and analysis centers and organizations.
  - **ICOAST**. This platform is used to share classified cyber threat indicators among federal agencies at the top secret security level. The Intelligence Community Security Coordination Center within ODNI maintains ICOAST. According to its director, ICOAST has allowed cyber analysts to more effectively share cybersecurity threat intelligence and defensive measures in a timely, adequate, and appropriate manner.
  - **Shared Cybersecurity Services**. This service provides agencies access to commercial cybersecurity threat intelligence vendors and associated offerings at no cost. CISA contracts with various vendors that provide agencies with cybersecurity threat intelligence platforms and feed integration capabilities, data aggregation and enrichment, intelligence sources (e.g., open source intelligence, public, and proprietary), reporting and requests for information support, analysis reports, and other services.

  By providing federal agencies access to trusted cybersecurity threat intelligence platforms, agencies can quickly adopt such platforms and

use their cyber threat information to identify, assess, monitor, and respond to cyber threats.

Resources Assist Agencies in Incident Prevention

Agencies need resources, including skilled staffing and funding, for their incident response programs.

Staffing. A key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce. According to NIST, an agency may structure its incident response team by using a centralized or a distributed approach or by using a coordinating team.[27] Further, incident response teams may use different staffing models with all government employees, or by partially or fully outsourcing its incident response work. In addition, NIST states that whichever approach an agency takes, a single employee (e.g., an incident manager), with one or more designated alternates should oversee incident response. Other incident response roles may include security operations center staff, engineers, cyber defense, forensic, and threat intelligence analysts.

Funding. Enhancing incident response capabilities such as increasing personnel, enhancing additional continuous monitoring, and acquiring detection tools requires funding. For example, for an agency to enhance its data logging capability, it may need to purchase additional storage capacity. The following sources of cybersecurity-related funding are available to agencies.

- The President's fiscal year 2023 budget included approximately $10.9 billion of budget authority for civilian cybersecurity-related activities including to support and upgrade federal civilian cybersecurity capabilities. This is an 11 percent increase reported from fiscal year 2022.
- The Technology Modernization Fund was established for technology-related activities, to improve IT, and to enhance cybersecurity across the federal government.[28] According to the General Services Administration, the fund has invested in projects that directly respond to the need to improve the nation's cybersecurity, as required by Executive Order 14028. In March 2021, the American Rescue Plan

[27]NIST SP 800-61, Revision 2.

[28]The provisions commonly referred to as the Modernizing Government Technology Act established the Technology Modernization Fund in the Department of the Treasury to provide transfers of amounts to agencies to help them improve, retire, or replace existing federal IT systems. Pub. L. No. 115-91, div. A, title X, subtitle G, § 1078, 131 Stat. 1586, 1589 (2017).

Act of 2021[29] appropriated $1 billion to the fund to address urgent IT modernization challenges, among other things.

- The American Rescue Plan Act of 2021 also provided $650 million to CISA for cybersecurity risk mitigation, of which CISA allocated $257 million to assist federal agencies with CDM and EDR efforts.
- The fiscal year 2023 President's Budget Request for CISA included $425 million for the CDM program, including $73 million to expand the EDR initiative across high-priority agency hosts and endpoints across federal civilian executive branch agencies.

Agencies Made Progress in Certain Incident Response Areas, but Have Not Met Event Logging Requirements

As noted earlier, the executive order and implementing guidance call for agencies to (1) standardize incident response procedures, (2) improve detection of vulnerabilities and incidents on federal networks, and (3) improve federal investigative and remediation capabilities (event logging). Federal agencies have made progress by (1) taking steps to standardize their incident response plans and (2) demonstrating improvement in their processes and capabilities for incident detection. However, many agencies have not met requirements for investigative and remediation (event logging) capabilities.

Agencies Are Taking Steps to Standardize Incident Response Plans and Processes

Agencies and CISA are taking steps to standardize cybersecurity incident response. First, CISA issued the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* in November 2021, providing the standardized procedures for agencies to use in incident response.[30]

In addition, as a result of the SolarWinds cyber incident, CFO Act agencies identified actions they intended to take to improve their incident

[29]On March 11, 2021, Congress and the President enacted legislation that appropriated $1 billion to be available until September 30, 2025, to carry out the purposes of the fund. American Rescue Plan Act of 2021, Pub. L. No. 117-2, title IV, § 4011, 135 Stat. 4, 80 (2021).

[30]Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* (November 2021).

response programs. Of the 23 CFO Act agencies, 18 compiled after actions or lessons learned reports.[31]

Specifically, 14 of 18 agencies' after actions or lessons learned reports identified needing to take action such as updating policies and procedures related to incident response security, event logging, auditing, and software patching. In March and April 2022, nine of those 14 agencies reported that they had assessed CISA's playbook against their agency incident response plans and updated or better aligned their plans in accordance with the playbook.[32] The remaining five agencies reported that they have plans to do the same or are in the process of doing so.

For the four agencies with after actions or lessons learned reports that did not identify the need to update policies and procedures, two stated that they had aligned the playbook with their agencies' incident response plans and two reported that they are in the process of doing so.

Of the remaining five agencies that did not complete an after action or lessons learned report, two reported they had integrated the playbook elements into their agency incident response plans and three reported that they are in the process of incorporating the playbook into their plans. According to OMB, as of October 2022 all agencies reported that they had updated or better aligned their incident response plans with the playbook.

Agencies Substantially Completed Incident Response Preparation Activities, but Work Remains

According to CISA, agencies need to prepare for major incidents before they occur to mitigate any impact on the organization.[33] To prepare, agencies should complete activities[34] that contribute to their ability to:

[31]Eighteen of the 23 CFO Act agencies that we assessed completed and provided GAO after action reports for the SolarWinds event. The remaining five agencies did not create after action reports because they did not utilize, or never had, affected versions of SolarWinds Orion on their networks or determined a report was not necessary.

[32]The playbook is intended to provide a standardized response process for cybersecurity incidents and describe the process and completion through the five incident response phases as defined in NIST SP 800-61, Revision 2, including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. In addition, it includes a checklist of preparation phase activities agencies should take to prepare for major incidents before they occur to mitigate any impact on the agency.

[33]Preparation is one of the five phases of the playbook.

[34]These activities are listed in table 7.

- document and understand policies and procedures for incident response (Policies and Procedures);
- deploy tools to detect suspicious and malicious activity (Instrumentation);
- establish staffing plans and educate users on cyber threats and notification procedures (Train Response Personnel);
- leverage cyber threat intelligence to proactively identify potential malicious activity (Cyber Threat Intelligence);
- establish local and cross-agency communication procedures and mechanisms for coordinating major incidents (Communications and Logistics);
- take steps to ensure that incident response and defensive systems and processes will be operational during an attack (Operational Security);
- implement capabilities to contain, replicate, analyze, reconstitute, and document compromised hosts (Technical Infrastructure); and
- leverage threat intelligence to create rules and signatures to identify the activity associated with the incident and to scope its reach (Detect Activity).

All 23 agencies that we assessed demonstrated that they substantially completed the playbook's incident response preparation activities.[35] OMB's annual FISMA report for fiscal year 2022 reported that agencies had evaluated the playbook against their incident response procedures and made enhancements.[36]

However, no agency fully completed all of the activities. In part, this was because the playbook did not provide enough detail or guidance to agencies for some of the preparation activities.[37] According to the executive order, standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of

[35]We reviewed and analyzed agency responses and documentation to determine completion of key selected playbook cybersecurity incident response preparation phase activities by the 23 civilian CFO Act agencies We excluded DOD from our combined analysis as the playbook applies to federal civilian executive branch agencies.

[36]OMB, *Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2022* (Washington, D.C.: May 1, 2023).

[37]The playbook also included the preparation activity of ensuring that event logging is in compliance with Executive Order 14028 (to include related requirements issued by OMB). As of August 2023, only three of the 23 civilian CFO Act agencies were in compliance.

agencies' progress toward successful responses. However, agencies noted the following activities were unclear:

- Within the Train Response Personnel activity, the playbook directs agencies to conduct regular recovery exercises to test full organizational continuity of operations plan (COOP), including failover, backup, and recovery of systems to be sure these work as planned. According to DHS, COOP planning can ensure continued performance of essential functions and reduce or mitigate disruptions to operations. However, the playbook does not provide guidance to agencies on what is considered "regular" for holding exercises, nor the criteria used to develop this playbook preparation activity.

  Agencies did not interpret the playbook activities in the same way as they related to COOP testing and took different approaches to addressing the guidance. For example, eight agency officials cited participation in a DHS-led exercise that tested COOP, including failover, backup, and recovery of systems, while other officials stated that their agency does not require contingency plan testing to include recovery exercises of full failover, backup, and recovery of systems or their agency does not conduct organization COOP activities as defined in this preparation activity.[38]

- Within the Communications and Logistics activity, the playbook only specifies that agencies designate and provide a single reporting point of contact to communicate with CISA. However, NIST Special Publication 800-61 states that each federal civilian agency must designate a primary and secondary point of contact with DHS and report all incidents consistent with the agency's incident response policy. CISA officials stated that they intend to update the preparation checklist to describe the need for a primary and secondary point of contact, but that CISA was initially focused on ensuring that every agency has at least one named point of contact.

Until CISA provides clear guidance to agencies regarding how to implement all incident response preparation activities in the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*, agencies are at risk of not being fully prepared to respond to major cybersecurity incidents, potentially increasing impact to the organization.

[38]Eagle Horizon is an annual continuity exercise for all federal executive branch departments and agencies coordinated by DHS through the Federal Emergency Management Agency and its National Continuity Programs Directorate. The exercise requires each federal executive branch department and agency to test their COOP.

Agencies Have Demonstrated Improvement in Their Processes and Capabilities for Incident Detection

Agencies Have Made Progress in Processes for Incident Detection

Agencies also demonstrated progress in their annual IG metrics ratings for the respond function of the NIST cybersecurity framework.[39] This is the function that includes incident response. Specifically, the IGs assessed agencies on the overall maturity of their processes for incident detection and analysis, among other things.[40] For fiscal year 2022, all agencies were at a level 3 or higher and 15 were at level 4 or higher. In addition, from fiscal year 2020 to fiscal year 2022, six agencies' ratings for the IG metric improved, 15 stayed the same, and two declined. Table 3 shows the maturity ratings for the respond function for the 23 agencies from fiscal year 2020 to fiscal year 2022.

Table 3: Inspector General (IG) Maturity Level for the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Programs

Agency	Fiscal Year 2020	Fiscal Year 2021	Fiscal Year 2022
Department of Agriculture	4	3	4
Department of Commerce	2	3	3
Department of Education	3	3	4
Department of Energy	4	4	3
Department of Health and Human Services	3	3	3
Department of Homeland Security	3	3	4

[39]Agencies and their IGs use the NIST Cybersecurity Framework in reporting on the effectiveness of agency information security policies and practices. The framework is based on five core security functions, the *respond* function includes developing and implementing appropriate activities to take action regarding a detected cybersecurity incident.

[40]IGs are required to assess the effectiveness of information security programs on a five-level maturity model (ad hoc, defined, consistently implemented, managed and measurable, and optimized). Level 4 is considered Managed and Measurable, where agency information security programs are considered operating at an effective level of security. Level 3 is considered Consistently Implemented, where information security programs are considered to consistently implemented but measures are lacking.

Agency	Fiscal Year 2020	Fiscal Year 2021	Fiscal Year 2022
Department of Housing and Urban Development	3	3	3
Department of Justice	4	4	5
Department of Labor	4	4	4
Department of State	4	4	4
Department of the Interior	4	3	3
Department of the Treasury	4	3	4
Department of Transportation	3	3	3
Department of Veterans Affairs	4	4	4
Environmental Protection Agency	3	3	3
General Services Administration	4	5	5
National Aeronautics and Space Administration	3	3	3
National Science Foundation	4	4	4
Nuclear Regulatory Commission	4	4	4
Office of Personnel Management	4	4	4
Small Business Administration	4	4	4
Social Security Administration	4	4	4
U.S. Agency for International Development	4	4	5

Key: The five maturity levels, from the least to the most mature, are: Level 1 (Ad Hoc); Level 2 (Defined); Level 3 (Consistently Implemented); Level 4 (Managed and Measurable); and Level 5 (Optimized).

Sources: GAO analysis of inspector general report data and OMB's FISMA reports to Congress. | GAO-24-105658

Note: As reported in the IGs' Federal Information Security Modernization Act of 2014 Fiscal Year 2020-2022 assessments.

Agencies Have Made Progress in Addressing Detection Capability Requirements

CISA and agencies have taken several actions to improve the federal government's incident response detection capabilities. Specifically, agencies have made progress addressing CDM requirements and are working toward full deployment of EDR solutions.

Agencies Have Made Progress Addressing CDM Requirements

According to Executive Order 14028, the federal government should use all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. In response to the executive order, agencies and CISA were to take specific actions to address CDM requirements.

Agencies have made progress in addressing these requirements. Table 4 describes the key CDM requirements along with the status of completion of each.

Table 4: Federal Agencies' Progress in Meeting Key Continuous Diagnostics and Mitigation Requirements

Source and title	Requirement	Status of completion
The White House, Executive Order 14028	Agencies are to establish or update memoranda of agreement (MOA) with Cybersecurity and Infrastructure Security Agency (CISA) for the continuous diagnostics and mitigation (CDM) program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law.	Complete. All 23 agencies have a signed CDM MOA and are sharing object level data (or data from or about specific devices connected to the agency network, users on that network, or information about the environment in which the network operates).
Office of Management and Budget (OMB), M-22-05	CISA is to perform a program review of CDM and incorporate lessons learned into a strategy to continue improving the program for fiscal year 2022.	Complete. According to CISA, as of August 2023, it had provided the program review to OMB for approval.
	CISA, in coordination with OMB and National Institute of Standards and Technology, is to develop a strategy to continue to evolve machine-readable data standards for cybersecurity performance and compliance data through CDM (or a successor process).	Complete. CISA completed the strategy in June 2022. According to OMB, it began working with CISA in April 2023 to automate collection of certain data sources into the fiscal year 2023 Federal Information Security Modernization Act of 2014 Chief Information Officer metrics.
CISA Binding Operational Directive, 23-01	By April 3, 2023, agencies and CISA, through the CDM program, are to deploy an updated CDM dashboard configuration that enables access to object-level vulnerability enumeration data for CISA analysts, as authorized in the Executive Order on *Improving the Nation's Cybersecurity*.	Ongoing. CISA stated that it made the new CDM dashboard configurations available to the agencies' CDM integrators on April 19, 2023. Agencies have 6 months to implement the new dashboard configurations. According to CISA, as of August 2023, 11 agencies had deployed the updated configuration.[a]
Office of Management and Budget, M-23-03	By January 2023, CISA is to begin providing OMB monthly data on CDM implementation progress by all federal agencies.	Ongoing. CISA provides CDM updates to OMB at biweekly meetings and provides a report to OMB on a bimonthly basis.

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

[a]On November 8, 2023, a CISA official stated that 89 federal agencies had deployed the updated configuration but did not indicate which of those were CFO Act agencies.

Agencies Have Advanced Endpoint Detection and Response Capabilities

The executive order required federal civilian executive branch agencies to adopt a robust EDR solution as part of the shift in cyber defense from a reactive to a proactive posture. In addition, OMB also required agencies to report on their EDR solutions.

Federal agencies have made progress in advancing their EDR capabilities. Table 5 describes the key EDR requirements and the status of completion of each.

Table 5: Federal Agencies' Progress in Meeting Key Endpoint Detection and Response (EDR) Requirements

Source and title	Requirement	Status of completion
The White House, Executive Order 14028	Agencies are to deploy an EDR initiative to support proactive detection of cybersecurity incidents within federal government infrastructure, active cyber hunting, and containment and remediation.	Ongoing. As of March 2023, the Cybersecurity and Infrastructure Security Agency (CISA) reported that all 23 agencies had identified an enterprise EDR tool and have begun working toward deploying the EDR tool.
Office of Management and Budget (OMB), M-22-01	Federal agencies are to conduct an analysis, in coordination with CISA, to assess the current status of their EDR capabilities by identifying any gaps in existing EDR deployments.	Complete. All 23 agencies conducted an analysis and identified gaps in existing EDR deployments if they existed. For those agencies without gaps, they informed CISA they had no gaps at that time.
	Within 90 days CISA shall develop a process for continuous performance monitoring to help agencies ensure that EDR solutions are deployed and operate in a manner that will detect and respond to common threats.	Complete. CISA included a process for continuous performance monitoring of EDR tools in the Federal Civilian Executive Branch Playbook on Best Practice Considerations for Endpoint Detection and Response Solutions Deployment and Implementation (December 12, 2022). To continuously monitor health and visibility coverage of the EDR solution, CISA will utilize various data points and telemetry reported through the Continuous Diagnostics and Mitigation program.
	Within 90 days CISA, in coordination with the Chief Information Officer (CIO) Council, shall provide recommendations to OMB on ways to further accelerate government-wide EDR efforts.	Complete. CISA completed and submitted its Recommendations for Accelerating Adoption of Endpoint Detection and Response Solutions to OMB following coordination with the Chief Information Security Officer Council's CISA Engagement Working Group.
	Within 90 days, CISA, in coordination with the CIO Council, shall develop and publish a technical reference architecture and maturity model for agency consumption.	Complete. CISA completed the technical reference architecture and maturity model and included them within the Federal Civilian Executive Branch Centralized Visibility Concept of Operations.
	Within 180 days, CISA, in coordination with the CIO Council, shall develop a playbook of best practices for EDR solution deployments to achieve government-wide operational visibility.	Complete. CISA stated that, in coordination with the CIO Council, it developed and published the Playbook on Best Practice Considerations for Endpoint Detection and Response Solutions Deployment and Implementation (December 12, 2022).

Source and title	Requirement	Status of completion
Office of Management and Budget, M-23-03	Federal agencies are to report EDR coverage of at least 80 percent of government-furnished equipment by the end of fiscal year 2023.	Ongoing. According to CISA, as of August 2023, 16 agencies reported EDR coverage on at least 80 percent of endpoints.

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

Most Agencies Have Not Met Event Logging Capability Requirements

OMB issued an August 2021 memorandum, as directed by the executive order, that stated that information from logs on federal information systems is invaluable in the detection, investigation, and remediation of cyber threats.[41] The memorandum outlined a maturity model that agencies are to follow in order to enhance their event logging, log retention, and log management activities. The maturity model consists of four event logging tiers intended to help agencies prioritize their efforts and resources so that, over time, they will achieve full compliance with requirements for implementation, log categories, and centralized access.

Each tier has specific requirements for the information that agencies must collect, the acceptable formats for the required data, the minimum length of time that agencies must retain the data, and the criticality level that is based on the usefulness of the log data for threat detection.

Agencies were to reach the advanced (tier 3) level by August 2023. 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. The tier descriptions and number of agencies that had reached each tier as of August 2023 are shown in table 6.

Table 6: Agency Implementation of OMB Memorandum M-21-31 Event Logging Requirements (as of August 2023)

Event logging tier	Description	Due date	Number of agencies at tier
Not effective (0)	Logging requirements of highest criticality are either not met or are only partially met.	Not applicable	17
Basic (1)	Only logging requirements of highest criticality are met.	8/27/2022	3
Intermediate (2)	Logging requirements of highest and intermediate criticality are met.	2/27/2023	0
Advanced (3)	Logging requirements at all criticality levels are met.	8/27/2023	3

Source: GAO analysis of Office of Management and Budget (OMB) information. | GAO-24-105658

Note: Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: Aug. 27, 2021).

[41]OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: Aug. 27, 2021).

As shown in the table, as of August 2023, three agencies had met tier 3. These agencies were the Department of Agriculture (Agriculture), the National Science Foundation (NSF), and the Small Business Administration (SBA). Officials from SBA and Agriculture credited their agencies' successes to agency efforts that preceded the issuance of the OMB memorandum. Specifically, the SBA official stated that the agency had begun to streamline enterprise cybersecurity services, identified as a best practice within NIST's guidance on event logging. The Agriculture official stated that efforts the agency had undertaken to meet the security operations center consolidation requirements of a fiscal year 2018 OMB memorandum assisted in meeting the event logging requirements. Further, an official from NSF stated that the agency achieved success through close coordination and enhanced licensing with its security incident and event management provider.

However, as of August 2023, 17 agencies were at tier 0, and three agencies were at tier 1.[42] Further, officials stated their agencies were not expected to meet the tiers soon.[43] Specifically,

- two agencies estimated reaching tier 1 in fiscal year 2023 and another agency by fiscal year 2024, and
- seven agencies estimated not reaching tier 3 until between fiscal years 2024 and 2026,
- ten agencies did not provide an updated timeline on when they expect to ultimately reach tier 3.

Agency officials noted that although they had not reached the tiers at the scheduled timelines, they have nonetheless made progress since 2021. Specifically, agency officials cited the "all or nothing" nature of the

[42]Agencies that had reached tier 1 as of August 2023: the General Services Administration; the Social Security Administration; and the U.S. Agency for International Development. Agencies that were still at tier 0 as of August 2023: the Departments of Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the National Aeronautics and Space Administration; the Nuclear Regulatory Commission; and the Office of Personnel Management.

[43]In September 2023, the Office of Inspector General for the U.S. Agency for International Development (USAID) recommended that USAID's CIO fully implement event logging requirements in accordance with OMB memorandum M-21-31. The Office of the CIO agreed with the recommendation and stated that the agency will fully implement the event logging requirements with a targeted completion date of December 31, 2023. USAID OIG, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA,* A-000-23-004-C (Washington, D.C.: Sept. 8, 2023).

requirements, meaning even if a majority of systems had reached the tier 1 requirements, if all systems had not reached tier 1, the agency overall would be at tier 0. For example, one agency official stated that his agency was at 98 percent completion of requirements for tier 1, but overall was still at tier 0.

Most agencies have not been successful in meeting the requirements due, in part, to the inability to allocate funding and resources within the timelines that would be needed to meet the requirements established in the OMB memorandum. Specifically, agency officials stated that the 2-year timelines to meet the requirements created challenges in securing funding for the personnel, software licensing, and tools needed to fulfill the requirements. For example, 17 agency officials cited funding challenges or resource constraints. One agency official stated that its agency estimated that it would require more than 9 years or sufficient additional funding for contractors to account for the new workload needed to meet the event logging tiers.

Nonetheless, it is essential for agencies to meet the event logging tiers. Until agencies fully implement all event logging requirements in OMB guidance, there is increased risk that they will not have complete information from logs on their systems to detect, investigate, and remediate cyber threats.

Agencies Are Challenged in Fully Preparing to Respond to Cybersecurity Incidents, but Federal Efforts May Assist

Agencies described three key challenges that hindered their abilities to prepare fully to respond to cybersecurity incidents: lack of staff, technical challenges in event logging, and limitations in cyber threat information sharing. Federal entities have initiated efforts that can assist in overcoming these challenges.

Agencies Reported a Lack of Staffing Needed to Support Incident Response Programs

More than half of the federal agencies in our review described challenges related to staffing. Specifically, 16 of 24 agencies reported needing additional staff or positions to carry out incident response activities. For example, these agencies mentioned a need for intelligence, threat, or forensic analysts as well as hunt teams. Six agencies also mentioned having unfilled positions within the security operations center, including leads, analysts, and supervisors.

In addition, several agencies noted a need for additional staff to meet the key cybersecurity incident response requirements. For example, eight of 23 agencies cited staffing as a gap or challenge in meeting event logging requirements.[44] Specifically, one agency official stated that additional staff will be required to manage the storage and analysis of the significant increase in data, estimating that the agency would need to triple the size of the current team responsible to ensure compliance with certain federal requirements.

There are both short-term and long-term efforts underway to address this challenge:

- As previously mentioned, CISA has a short-term offering that may be able to assist agencies with immediate cyber incident response staffing challenges. Specifically, CISA provides free assistance upon request to agencies with staffing shortages by providing onsite support to augment an agency's forensics efforts and investigate cyber incidents and any impacts on the agency. CISA officials reported that HIRT engaged with 14 agencies in fiscal year 2021 and with 11 agencies in fiscal year 2022 to provide assistance with incident response staffing challenges. In addition, CISA stated that it has efforts underway to increase its staff to support more concurrent engagements in the future.
- In the long term, federal efforts are underway to address the national cybersecurity staffing shortage. Specifically, the National Cybersecurity Strategy released in March 2023 included an objective to develop a sub-strategy aimed at addressing the challenges around the federal cyber workforce.[45] This sub-strategy, the National Cyber Workforce and Education Strategy, released in July 2023, is to assist in strengthening and diversifying the federal cyber workforce to address the unique challenges the public sector faces in recruiting, retaining, and developing the talent and capacity needed to protect federal data and IT infrastructure.[46]

  The sub-strategy, among other things, highlights the need to expand and enhance the nation's cyber workforce and strengthen the federal

[44]We did not include DOD in this analysis because it was not subject to the requirements in our review.

[45]The White House, *National Cybersecurity Strategy* (Washington, D.C., Mar 1, 2023).

[46]Office of the National Cyber Director Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent* (Washington, D.C.: July 31, 2023).

cyber workforce.[47] In particular, to overcome hiring delays, the sub-strategy states that there is an initiative to improve personnel vetting, reduce the time required to bring new hires onboard, and better enable the mobility of the federal workforce. If these efforts are implemented, they may assist agencies in addressing their workforce challenges.

We have previously reported that federal agencies varied widely in their efforts to implement key IT workforce planning activities that are critical to ensuring that agencies have the staff they need to support their missions. Effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary knowledge, skills, and abilities to execute a range of management functions that support agencies' missions and goals. Thus, agencies should continue to work toward fully implementing these recommendations which may assist agencies as they work toward addressing their staffing challenges.

Agencies Reported Technical Challenges in Meeting Event Logging Requirements

As previously mentioned, 20 of the 23 agencies had not met the tiered event logging requirements established by OMB. Agencies also reported technical challenges in meeting the event logging requirements. Specifically, 12 agencies stated that gaps in technology or complexities with existing technical environments (e.g., legacy systems) proved challenging in meeting the requirements.

In addition, 17 agencies cited the need for increased storage capacity to meet event logging requirements. For example, to meet event logging levels, some agencies may need to increase storage capacity for logs. This may be due to a need to capture more granular level details or to capture data on events that were not previously required or captured. One agency official stated that his agency currently collects over 7 terabytes of log data per day with a retention of 1 year. The official stated that in order to be compliant with current logging data requirements, the agency would need to expand logging to 70 terabytes per day. Another agency official stated that his agency already collects over 13 billion logs daily, accounting for almost 15 terabytes of data per day.[48]

[47]In August 2023, CISA released its fiscal year 2024-2026 Cybersecurity Strategic Plan that states that CISA will work closely with the Office of the National Cyber Director to implement a national cybersecurity workforce and education strategy.

[48]A terabyte is a unit of computer information consisting of about 1,000,000,000,000 bytes.

CISA and OMB have provided assistance to agencies in implementing event logging requirements, in part through CyberStat.[49] For example, in September 2021, CyberStat hosted a workshop on logging requirements. In addition, according to officials, CISA gathers agency questions through technical engagements and assistance, and then seeks responses from subject matter experts and posts the responses on their webpage for all interested agencies to use. In December 2022, CISA hosted another CyberStat workshop and released guidance to assist agencies in implementing OMB's event logging memorandum. According to the guidance, it may assist agencies in prioritizing the deployment, collection, and storage requirements as well as assist OMB and CISA in tracking agency progress in achieving event logging maturity.

Further, an OMB official stated that the agency has provided support to agencies by meeting with the private sector to better understand the costs of short and long-term configurations. They also noted that OMB has helped agencies with budgeting for event logging.

Agencies Reported Limitations in Cyber Threat Intelligence Data Sharing

Agencies identified a number of challenges in the collection, aggregation, or sharing of cyber threat intelligence data.[50] Fourteen of the 24 agencies reported classification challenges in collecting, aggregating and sharing cyber threat intelligence data. For example, one agency official stated that it is a challenge to take an indicator of compromise from a classified network to use on an unclassified network. Without those indicators, an analyst's ability to quickly utilize the potential threat information and take action to prevent or mitigate effects from a cybersecurity threat may be hindered. In addition, officials from at least two agencies stated a challenge around not having enough cleared staff to access and analyze classified data.

Further, 13 agencies reported challenges with the quality or the timeliness of the data being shared. For example, agency officials at nine agencies stated that they receive a large volume of cyber threat intelligence from a variety of sources, including AIS, which can result in redundant

[49]CyberStat is a CISA program that offers workshops and guidance to address common problems across the federal enterprise.

[50]We recently reported on the challenges to cyber threat information sharing, specifically among federal agencies and critical infrastructure owners and operators. See GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Challenges, Performance Measures, and Methods*, GAO-23-105468 (Washington, D.C.: Sept. 26, 2023).

information or information that may be out-of-date by the time the analysts can complete the analysis of the data.

The 2021 Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015 highlighted similar challenges to sharing cyber threat information. Specifically, the report described classification concerns, stating that over-classification may significantly delay or halt the ability to analyze shared indicators due to the amount of effort necessary to declassify and transfer the indicators to unclassified systems. In addition, regarding data quality, the report stated that much of the cyber threat indicator and defensive measure information received through AIS did not contain the necessary context or that it contained redundant indicators because it did not remove identical ones uploaded by multiple entities.

There are several federal actions under way to address this challenge:

- Officials from the Defense Information Systems Agency stated in the joint report that they have collaborated with other agencies to find solutions to minimize over-classification and have instituted a process to manually review indicators provided to other federal entities and insert additional context into cyber threat indicators in AIS.
- A CISA official stated that the agency is working with ODNI and with the Intelligence Community Sector Coordinating Council on a plan to make declassifying and disseminating unclassified elements of cyber threat information that are contained within classified systems accessible and actionable.
- According to CISA officials, CISA has made enhancements to its AIS platform intended to address some of the challenges identified with the quality and the timeliness of the data. In addition, CISA officials reported that the agency is working on updating documentation that outlines how to connect to AIS and streamline the onboarding process to AIS. As a next step, CISA officials stated that they plan to prioritize outreach to focus on data hubs and entities that are mature enough to share data with CISA.
- CISA has agreements with 15 third party (or commercial) threat intelligence companies to provide built-in AIS data streams in their threat intelligence platforms to agencies. These partnerships allow AIS data to be more accessible to agencies that cannot connect to AIS due to technical challenges.

CISA officials stated that CISA is planning to roll out the first phase of a new threat intelligence platform offering, Cyber Threat Intelligence as a Service, to federal departments and agencies in fiscal year 2024. The platform will be centrally funded through CISA, providing free threat intelligence information and downstream AIS data to participating agencies. This would minimize costs to agencies, as they no longer would need to build out the technical infrastructure required to integrate with AIS.

Conclusions

Since the SolarWinds cyber incident, all civilian CFO Act agencies and CISA made progress in improving incident response capabilities by standardizing incident response plans and processes and enhancing incident response detection capabilities. CISA issued the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* and all agencies demonstrated that they had substantially completed the cybersecurity incident response preparation activities listed within the playbook. However, the guidance on completing certain incident response preparation activities, such as designating primary and secondary points of contact and on COOP testing, did not provide enough detail to agencies. A playbook with additional clarity from CISA could assist agencies in better implementing cybersecurity incident response activities.

In addition, CISA and agencies have made progress addressing CDM requirements and are working toward full deployment of EDR solutions. However, most agencies have not completed incident response event logging requirements. Until agencies implement all event logging requirements outlined in OMB guidance, there is increased risk that they will not have complete information on their efforts to detect, investigate, and remediate cyber threats. Moreover, the federal government as a whole may lack critical information and insights for identifying potentially significant cyber threats.

Recommendations for Executive Action

We are making 20 recommendations to the heads of federal agencies:

The Director of CISA should ensure that when the agency updates the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* that it provides additional detail to federal agencies on COOP planning and includes the requirement to provide both primary and secondary points of contact to CISA. (Recommendation 1)

The Secretary of Commerce should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 2)

The Secretary of Education should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 3)

The Secretary of Energy should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 4)

The Secretary of Health and Human Services should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 5)

The Secretary of Homeland Security should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 6)

The Secretary of Housing and Urban Development should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 7)

The Secretary of the Interior should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 8)

The Attorney General should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 9)

The Secretary of Labor should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 10)

The Secretary of State should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 11)

The Secretary of Transportation should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 12)

The Secretary of the Treasury should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 13)

The Secretary of Veterans Affairs should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 14)

The Administrator of the Environmental Protection Agency should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 15)

The Administrator of the General Services Administration should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 16)

The Administrator of the National Aeronautics and Space Administration should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 17)

The Chairman of the Nuclear Regulatory Commission should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 18)

The Director of the Office of Personnel Management should ensure that the agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 19)

The Commissioner of the Social Security Administration should ensure that the agency fully implements all event logging requirements as directed OMB guidance. (Recommendation 20)

Agency Comments and Our Evaluation

We provided a draft of this report to 24 agencies and OMB for their review and comment. Of the 19 agencies[51] to which we made recommendations in this report,16 agencies agreed with the recommendations and three agencies neither agreed nor disagreed with the recommendations.

In addition, of the six agencies to which we did not make recommendations in this report, one (the U.S. Agency for International

[51]Because CISA is a component of DHS, two of our recommendations went to the department for review and comment.

Development (USAID)) provided comments on the report and the remaining five (Agriculture, DOD, NSF, OMB, and SBA) responded that they did not have any comments on the report. We also received technical comments from three agencies, which we have incorporated into the report, as appropriate.

The following 16 agencies agreed with our recommendations:

- In written comments, reprinted in appendix II, the Department of Commerce concurred with our recommendation.
- In written comments, reprinted in appendix III, the Department of Education concurred with our recommendation and stated that it plans to address our recommendation by, among other things, using a risk-based prioritization approach to achieve each event logging level. It also noted certain challenges it faces, such as funding and the lack of storage space, storage type, and bandwidth.
- In written comments, reprinted in appendix IV, the Department of Energy concurred with our recommendation and stated that it plans to achieve compliance with OMB requirements where technically feasible by 2028.
- In written comments, reprinted in appendix V, the Department of Health and Human Services concurred with our recommendation and stated that it plans to address our recommendation by, among other things, balancing future actions with the projected costs associated with meeting the requirements. It also noted that updated guidance that identifies the data logs CISA deems critical to incident response activities would be beneficial.
- In written comments, reprinted in appendix VI, DHS concurred with our recommendations.
- In written comments, reprinted in appendix VII, the Department of the Interior concurred with our recommendation and stated that it plans to address our recommendation by, among other things, continuing to work with OMB and updating its internal guidance to facilitate implementation, taking a prioritized approach to implement the requirements.
- In comments provided via email on November 10, 2023, an audit liaison from the Justice Management Division at the Department of Justice stated that the agency agreed with our recommendation.
- In comments provided via email on November 13, 2023, an economist from the Office of the Assistant Secretary for Policy at the Department

of Labor stated that the agency agreed with our recommendation. The official added that the agency plans to fully implement all event logging requirements as directed by OMB guidance by September 30, 2024.

- In comments provided via email on November 8, 2023, a management analyst from the Office of the Assistant Secretary for Administration at the Department of Transportation stated that the agency agreed with our recommendation.
- In written comments, reprinted in appendix VIII, the Department of Veterans Affairs concurred with our recommendation and stated that it plans to address our recommendation by, among other things, prioritizing efforts to meet all requirements.
- In written comments, reprinted in appendix IX, the Environmental Protection Agency concurred with our recommendation and stated that it plans to address our recommendation and estimates completing all requirements by August 15, 2024.
- In written comments, reprinted in appendix X, the General Services Administration concurred with our recommendation and stated that it is developing a plan to take appropriate action.
- In written comments, reprinted in appendix XI, the National Aeronautics and Space Administration concurred with our recommendation and stated that it plans to address our recommendation by, among other things, creating a comprehensive plan to address all event logging requirements under a recently established Cybersecurity Improvement Portfolio. It also noted certain challenges it faces, such as data integration into the agency's uniquely designed systems and resource constraints.
- In written comments, reprinted in appendix XII, the Nuclear Regulatory Commission concurred with our recommendation.
- In written comments, reprinted in appendix XIII, the Office of Personnel Management concurred with our recommendation and stated that it plans to address our recommendation by, among other things, prioritizing projects and initiatives but noted limited available resources including funding.
- In written comments, reprinted in appendix XIV, the Social Security Administration concurred with our recommendation.

Three agencies provided comments but did not state whether they agreed or disagreed with our recommendations:

- In comments provided via email on November 9, 2023, an audit liaison from the Office of the Chief Information Officer at the Department of Housing and Urban Development stated that the agency is currently working with agency IT stakeholders and administrators to meet OMB's logging requirements. The official also noted that the agency has procured several new tools, such as a new Security Information and Event Management tool and a User and Entity Behavioral Analytics platform.
- In written comments, reprinted in appendix XV, the Department of State noted that it plans to address our recommendation by, among other things, continuing its efforts through an enterprise-wide project that enables the processing, collection, and storage of data to meet the requirements.
- In comments provided via email on October 12, 2023, an audit liaison from the Office of the Chief Information Officer at the Department of the Treasury stated that the agency acknowledged its recommendation.

Regarding USAID, the draft report also contained a recommendation to the agency. However, during the comment period, USAID informed us that in September 2023, its Office of Inspector General had issued the same recommendation on event logging which USAID stated it planned to address. We reviewed the USAID Office of Inspector General recommendation and determined that it met the same intent as our recommendation. Therefore, we removed the recommendation to USAID. USAID's comments are reprinted in appendix XVI.

We are sending copies of this report to the appropriate congressional committees, the heads of the 24 CFO Act agencies, the Director of OMB, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be

found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix XVII.

Sincerely yours,

Jennifer R. Franks, Director
Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to: (1) describe the capabilities federal agencies rely upon to prepare and respond to cybersecurity incidents; (2) evaluate the extent to which federal agencies have made progress in preparing for cybersecurity incident response activities since the issuance of Executive Order 14028;[1] and (3) describe the challenges federal agencies face in preparing for cybersecurity incident response and what federal efforts, if any, can assist agencies with these challenges.

The scope of our review included:

- the 24 Chief Financial Officers (CFO) Act of 1990 agencies;[2]
- the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), as CISA is the lead agency for asset response activities across the federal government and is responsible for coordinating federal agencies' defense against cyberattacks; and
- the Office of Management and Budget (OMB), as OMB oversees federal agencies information security policies and practices and issues guidance to federal agencies.

To address the first objective, we reviewed documentation from the 24 CFO Act agencies, CISA, and National Institute of Standards and Technology (NIST) to identify the range of cybersecurity incident response tools, services, and resources agencies have in place. Such documentation included federal incident response guidance, agencies' incident response staffing plans, and budget requests and funding sources for cybersecurity incident response enhancements. Furthermore, we interviewed officials from the 24 CFO Act agencies, CISA, and OMB.

[1]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[2]The Chief Financial Officers (CFO) Act of 1990 established a CFO position at major federal agencies, referred to as CFO Act agencies. There are 24 agencies identified in the CFO Act: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. The Department of Defense was not included in the analysis we performed for our second objective as the requirements did not pertain to them.

To address the second objective, we identified key requirements within Executive Order 14028, associated OMB memoranda, and a CISA Binding Operational Directive. These documents dictate that federal agencies are to make improvements to federal cybersecurity incident response standardization, detection, and remediation efforts, such as endpoint detection and response,[3] continuous diagnostics and mitigation,[4] and event logging.[5] We reviewed and analyzed documentation from 23 civilian agencies and CISA to assess their progress in meeting key requirements.[6] Such documentation included agencies' gap analyses and implementation plans in response to OMB memoranda. In addition, we reviewed documentation that OMB directed CISA to complete, such as a CDM strategy document and an EDR concept of operations document. We also interviewed relevant agency officials.

Regarding standardization, we identified that the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*[7] (hereinafter referred to as the playbook) defined procedures federal agencies are to use in planning and conducting cybersecurity incident response activities.[8] In addition, we reviewed applicable NIST guidance for procedures agencies are to implement.

We then selected and compiled key incident response activities into a questionnaire. The questionnaire included questions on agencies' incident response activities and corresponding requests for

[3]OMB, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,* M-22-01 (Washington, D.C.: Oct. 8, 2021).

[4]OMB*, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (M-22-05) (Washington, D.C.: Dec. 6, 2021); and *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements,* M-23-03 (Dec. 2, 2022, rescinded M-22-05).

[5]OMB, *Improving the Federal Government's Investigative and Remediation Capabilities* Related to Cybersecurity Incidents, M-21-31 (Washington, D.C.: Aug. 27, 2021).

[6]We excluded the Department of Defense from our analysis using the playbook, as the playbook applies to federal civilian executive branch agencies.

[7]Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* (November 2021).

[8]Executive Order 14028 directed DHS, via CISA, to develop a standard set of operational procedures (the playbook) to be used by federal civilian executive branch agencies in planning and conducting cybersecurity vulnerability and incident response activities.

documentation for agencies' cybersecurity incident response policies, procedures, and plans.[9] We then reviewed and analyzed agency responses to the questionnaire and supporting documentation to determine completion of key selected playbook cybersecurity incident response preparation phase activities by the 23 civilian CFO Act agencies. Those selected activities are listed below in table 7.

Table 7: Selected Key Cybersecurity Incident Response Preparation Activities

Preparation category	Activity
Policies and Procedures	
	Document agency incident response plan with procedures for escalating and reporting major incidents and those with impact on agency mission
	Document procedure for designating agency incident coordination lead
	Identify key incident response personnel and responsibilities
	Identify system owners and Information System Security Officers
	Identify system IPs, system security plan, system/enclave boundaries, mission essential status, etc.
	Document contingency plan for additional resourcing or "surge support" with assigned roles and responsibilities[a]
Instrumentation	
	Implement detection and monitoring capabilities (e.g., antivirus software, end point detection and response solutions, data loss prevention capabilities, intrusion detection and prevention systems, audit logs network flows, packet captures, and security information and event management systems)
	Establish a baseline for systems and networks to understand what "normal" activity is to enable defenders to identify any deviations
	Implement EINSTEIN capabilities
	Implement continuous diagnostics and mitigation capabilities
	Ensure logging, log retention, and log management comply with Executive Order 14028, Sec 8
Train Response Personnel	
	Train and exercise agency and staffing personnel to prepare for major incidents
	Conduct recovery exercises to test full organizational continuity of operations plan (failover, backup, and recovery systems)[a]
Cyber Threat Intelligence	
	Monitor intelligence feeds for threat or vulnerability advisories from a variety of sources: government, trusted partners, open source, and commercial entities
	Integrate threat feeds into security information and event management system and other defensive capabilities to identify and block known malicious behavior

[9]The playbook's incident response preparation phase is organized into nine categories: Policies and Procedures, Instrumentation, Trained Response Personnel, Cyber Threat Intelligence, Active Defense, Communications and Logistics, Operational Security, Technical Infrastructure, and Detect Activity.

Preparation category	Activity
	Analyze suspicious activity reports from users, contractors and information and communication technology service providers; or incident reports from other internal or external organizational components
	Collect incident data (indicators, countermeasures, and tactics, techniques, and procedures) and share with Cybersecurity and Infrastructure Security Agency (CISA) and other partners (law enforcement, etc.)
	Set up CISA Automated Indicator Sharing or share via Cyber Threat Indicator and Defensive Measures Submission System
Communication and Logistics	
	Establish local and cross-agency communication procedures and mechanisms for coordinating major incidents with CISA
	Establish a communications channels (chat rooms and phone bridges) and methods for out-of-band coordination
	Designate CISA primary and secondary reporting point of contact[a]
	Define methods for handing classified information and data, if required
Operational Security	
	Segment and manage security operations center systems separately from broader enterprise IT systems
	Manage sensors and security devices via out-of-band means (network, etc.)
	Develop method to notify users of compromised systems via phone rather than email
	Use hardened workstations to conduct monitoring and response activities
	Ensure that defensive systems have robust backup and recovery processes
	Implement processes to avoid “tipping off” an attacker to reduce likelihood of detection of incident response-sensitive information (e.g., do not submit malware samples to a public analysis service or notify users of compromised systems via email)
Technical Infrastructure	
	Establish secure storage (i.e., only accessible by incident responders) for incident data and reporting
	Implement capabilities to contain, replicate, analyze, and reconstitute compromised hosts
	Deploy tools to collect forensic evidence such as disk and active memory imaging
	Implement capability to handle/detonate malware, sandbox software, and other analysis tools
	Implement a ticketing or case management system
Detect Activity	
	Implement security information and event management systems and sensor rules and signatures to search for indicators of compromise
	Analyze logs and alerts for signs of suspicious or malicious activity

Sources: GAO summary of information from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST). | GAO-24-105658

Note: CISA, *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* (November 2021); National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2 (Gaithersburg, MD: August 2012).

[a]We did not include the activity in an agency’s overall assessment.

Then, based on the number of completed activities, we determined the overall assessment rating of each agency by assigning one of the five assessment levels:

- Fully Completed. The agency provided evidence that demonstrated completion of all selected playbook activities.
- Substantially Completed. The agency provided evidence that demonstrated completion of a large portion of the selected playbook activities.
- Partially Completed. The agency provided evidence that demonstrated completion of about half of the selected playbook activities.
- Minimally Completed. The agency provided evidence that demonstrated completion of a small portion of the selected playbook activities.
- Not Completed. The agency did not provide evidence that demonstrated completion of any of the selected playbook activities.

In addition, we collected fiscal years 2020 through 2022 Federal Information Security Modernization Act of 2014 (FISMA) Inspector General (IG) Metrics data for the 23 CFO Act agencies because IGs use these metrics to assess and report on the effectiveness of their agencies' information security programs.[10] Specifically, we identified and analyzed the data from the FISMA IG metrics respond function of the NIST cybersecurity framework.[11]

Finally, we reviewed SolarWinds after action reports from the 23 agencies that produced them. In doing so, we identified the number of agencies that stated they needed to improve incident response policies and procedures. Because agencies were directed to use the *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks* as standard incident response procedures, we then compared those agencies' statements against the statements agencies made when asked

[10]The Department of Defense was excluded from our review and analysis of fiscal years 2020 through 2022 FISMA IG metrics data due to the sensitivity of the department's reports.

[11]Agencies and their IGs use the NIST Cybersecurity Framework in reporting on the effectiveness of agency information security policies and practices. The framework is based on five core security functions, the *respond* function includes developing and implementing appropriate activities to take action regarding a detected cybersecurity incident.

about whether and how they have implemented the incident response playbook.

To address the third objective, we interviewed officials from the 24 CFO Act agencies, CISA, and OMB. We requested information and documentation regarding challenges agencies have experienced with cybersecurity incident response. We also requested information regarding any challenges agencies have had in meeting executive requirements; receiving incident response assistance; and collecting, aggregating, and sharing cyber threat intelligence data.

We also requested information and documentation on what federal efforts could assist with the challenges. Through our interviews and data collection efforts, we categorized and grouped incident response preparation challenges. We also categorized and grouped assistance that CISA could provide to help overcome the challenges agencies identified.

We conducted this performance audit from January 2022 to December 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

November 16, 2023

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street NW Washington, DC 20548

Dear Director Franks,

Thank you for the opportunity to respond to the GAO draft report entitled GAO-24-105658, *Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements*.

The Department agrees with the recommendation and will prepare a formal action plan upon issuance of GAO's final report.

If you have any questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or mmausser@doc.gov.

Sincerely,

JEREMY PELTER
Digitally signed by JEREMY PELTER
Date: 2023.11.14 18:04:05 -05'00'

Jeremy Pelter
Deputy Assistant Secretary for Administration,
performing the non-exclusive functions and duties
of the Chief Financial Officer and
Assistant Secretary for Administration

Appendix III: Comments from the Department of Education

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

November 9, 2023

Jennifer R. Franks,
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Franks:

I am pleased to provide the U.S. Department of Education's (ED's or Department's) response to the Government Accountability Office's (GAO's) draft report, *Cybersecurity Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements* (GAO-24-105658). We understand that GAO conducted this audit as part of a multi-agency review to ensure that the Department fully implements all event logging requirements as directed by guidance from the Office of Management and Budget (OMB). We appreciate the opportunity to respond to the one recommendation for ED.

GAO Recommendation 3: The Secretary of Education should ensure that the Department of Education fully implements all event logging requirements as directed by OMB guidance.

Response: The Department concurs with this GAO recommendation and plans to implement event logging requirements, as resources permit. The Department has requested additional funds to address this recommendation for compliance under OMB Memorandum M-21-31 (OMB M-21-31) to ensure compliance with Event Logging level (EL). However, the full amount requested has not been granted to date. The Department has initiated a new blanket purchase agreement to address the larger task while still operating under this funding deficiency. Due to the Federal-wide funding deficiencies, however, the Department currently lacks approximately forty percent (40%) of the required funding to accomplish the defined logging goals for ELs 1 through 3, as further described below.

The Department's implementation strategy, at a high level, is to ingest all systems to an EL1 status, while prioritizing High Value Assets (HVA), using a risk-based prioritization approach. Once all ED systems are considered EL1, the next objective would be EL2, using the same strategy and prioritization.

The Department faces additional issues and challenges to meet the OMB M-21-31 mandate as it relates to EL3. The primary challenge with EL3 is related to storage space, storage type, and the bandwidth required to meet the seventy-two (72) hours of packet capture logging. This EL3 requirement entails managing massive amounts of data that need to be reviewed, stored, and made available for stakeholder consumption.

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

Challenges and risks that have been identified to implement EL3 logging maturity include:

- OMB M-21-31 requires seventy-two (72) hours of logging, which requires a very large amount of storage space that is not currently funded.
- ED's ability to sending the OMB M-21-31 required files to the ED Cyber Data Lake (EDCDL) creates projected bandwidth congestion.
- There are technical implementation challenges for publicly accessible, high availability encrypted traffic websites.
- Statistical data is generally prohibited from exposure to non-statistical personnel, including logging data. Technical controls for accessibility of statistical data in EDCDL are currently being investigated.

You may direct your questions to Mr. Christopher Erickson, Cyber Operations Branch Chief, at (202) 227-7159 or at Christopher.erickson@ed.gov.

Sincerely,

GARY STEVENS

Digitally signed by GARY STEVENS
Date: 2023.11.09 16:22:18 -05'00'

Luis Lopez
Chief Information Officer

Appendix IV: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

November 17, 2023

Jennifer R. Franks
Director of Center for Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Jennifer Franks:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a response to the Government Accountability Office's (GAO) Draft report titled, GAO Draft Report: *Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements (GAO 22-105658).* DOE concurs with the recommendation listed in the report and plans to achieve compliance with OMB requirements where technically feasible by the end of calendar year 2028.

The DOE Office of the Chief Information Officer oversees a highly federated environment with 53 Security Operation Centers (SOCs), 28 of which are federally operated and 25 are contractor-operated under management and operating (M&O) contract vehicles. The diverse missions (power transmission, headquarters business operations, nuclear security, environmental management, and open science) supported by these SOCs mean they operate under different risk profiles that drive historical investment priorities for these types of services, versus the common maturity model promoted in OMB M-21-31.

While the Department of Energy has made progress in improving enterprise logging capabilities, not all DOE sites achieved Event Logging (EL) tier 3 by meeting logging requirements at all criticality levels in FY23. In fiscal year 2023 4th quarter, 60 percent of DOE systems were reported at EL tiers 1-3, meeting or exceeding requirements for basic logging categories, minimum logging data, time standard, event forwarding, and passive DNS, while 40 percent were reported at EL tier 0, where logging requirements of highest criticality have not been fully implemented.

DOE is applying a risk-based approach to ensure that the highest risk issues are prioritized to have the most impact in reducing operational risks. DOE is continuing to track logging gaps, concerns, and timelines across its diverse risk profiles. DOE continues to face the challenges in implementing the requirements, as outlined in its September 28, 2022 report to OMB on Event Logging (EL) 1 implementation requirements. Meeting the EL3 target requires balancing mission and risk, adverse impacts on nuclear infrastructure, legacy research systems, and industrial control systems not capable of full implementation without significant disruption, and resources. Challenges include:

- Financial barriers to implement solutions.

- Single vendor solutions do not meet all the requirements specified in the memo, adding complexity and increasing cost.
- Lack of technical expertise and technical feasibility.
- Additional software, manpower, and technical expertise required to implement monitoring and the Security Orchestration Automation and Response (SOAR) capabilities needed once the logging solutions are in place.
- In some cases, such as supercomputing, implementing EL3 is not attainable due to the system architecture, the volume of data ingested, and the injection of latency into the system by logging tools. No vendor solution exists to support these environments.

GAO should direct any questions to Paul Selby, Deputy Chief Information Security Officer (CISO) and Deputy Chief Information Officer for Cybersecurity at Paul.Selby@hq.doe.gov

Sincerely,

Ann Dunkin
Chief Information Officer

Enclosure

Enclosure

MANAGEMENT RESPONSE
GAO Draft Report,
Federal Agencies Made Progress, but Need to Fully Implement
Incident Response Requirements (GAO-24-105658)

Recommendation 4: The Secretary of Energy should ensure that the Department of Energy fully implements all event logging requirements as directed by OMB guidance. (Recommendation 4)

Management Response: Concur

DOE is committed to continuing the maturing of its logging capabilities as expeditiously as possible with prioritization of its highest risk systems. Implementation of all event logging requirements as directed by OMB guidance is anticipated by 12/31/2028 for systems where it is technically feasible.

Estimated Completion Date: 12/31/2028

Appendix V: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

November 15, 2023

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements" (GAO-24-105658).**

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - CYBERSECURITY: FEDERAL AGENCIES MADE PROGRESS, BUT NEED TO FULLY IMPLEMENT INCIDENT RESPONSE REQUIREMENTS (GAO-24-105658)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 5
The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully implements all event logging requirements as directed by OMB guidance.

HHS Response
HHS concurs with GAO's recommendation.

HHS will continue to review GAO's recommendation and balance future actions with the projected significant costs of capturing and storing data. HHS will also consult with OMB and CISA as it continues to review this recommendation. Additionally, HHS will continue to review CISA M-21 31 Operational Guidance as this guidance focuses on logging sources that directly support incident response activities. HHS believes updated guidance that identifies those logs CISA deems critical to incident response activities would be beneficial in helping the Department implement event logging requirements, as is the ability to leverage a maturity scale that complies with the Zero Trust Maturity Model 2.0 which enables HHS and other agencies to properly assess maturity against established criteria.

Appendix VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 21, 2023

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-105658, "CYBERSECURITY: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements"

Dear Ms. Franks:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition that the Cybersecurity and Information Security Agency (CISA) is taking steps to standardize cybersecurity incident response with issuance of the "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks," dated November 2021.[1] GAO also acknowledged DHS' efforts to complete the playbook's incident response preparation activities.

On October 26, 2021, the DHS Management Directorate's (MGMT) Office of the Chief Information Officer (OCIO) submitted a response to the Office of Management and Budget (OMB) Memorandum M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," dated August 27, 2021.[2] Specifically, DHS OCIO developed a framework to conduct a self-

[1] https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
[2] https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf; OMB memorandum M-21-31 implements section 8 of Executive Order 10428, "Improving the Nation's Cybersecurity," dated May 12, 2021 for logging, log retention, and log management. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

evaluation across all Department Components to determine the current maturity and compliance levels for event logging (EL). The DHS self-evaluation method considered the maturity levels as cumulative capabilities in terms of reporting their compliance to OMB. As part of the self-evaluation, completed on October 8, 2021, DHS Components identified resource requirements needed to fill the gaps in their maturity to meet unfulfilled logging requirements aligned to the below OMB-defined EL maturity levels.

Further, DHS MGMT OCIO collected and reported to OMB the Department's EL maturity on a quarterly basis during fiscal year (FY) 2023 through OMB's Cyberscope tool for the Federal Information Security Modernization Act Reporting process. DHS regularly communicates key challenges to OMB with emphasis on budgetary concerns regarding its maturity efforts.

DHS intends to lead the Federal government by example when it comes to cybersecurity practices and the Administration's priorities. Accordingly, DHS is committed to developing its enterprise logging capabilities to ensure the Department leads the Federal government in cybersecurity and a strong incident response capability made possible by DHS' best practices in government logging maturity.

The draft report contained 21 recommendations, including two for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.11.21 07:41:15 -05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

Enclosure: Management Response to Recommendations Contained in GAO-24-105658

GAO recommended that the Director of CISA:

Recommendation 1: Ensure that when CISA updates the Federal Government Cybersecurity Incident & Vulnerability Response Playbooks that it provides additional detail to federal agencies on COOP [continuity of operations plan] planning and includes the requirement to provide both primary and secondary points of contact to CISA.

Response: Concur. As part of the annual product review lifecycle, CISA will assign resources to further clarify incident response preparation activities regarding COOP planning. This effort will be led by representatives of CISA's Threat Hunting sub-division, which will publish updates by the end of the second quarter of FY 2024. Estimated Completion Date (ECD): March 29, 2024.

GAO recommended that the Secretary of Homeland Security:

Recommendation 6: Ensure that the Department of Homeland Security fully implements all event logging requirements as directed by OMB guidance.

Response: Concur. On October 26, 2021, DHS MGMT OCIO sent OMB a memorandum, "DHS' Report on M-21-31, Investigative and Remediation Capabilities Related to Cybersecurity Incidents," which explained the framework DHS used to conduct a self-evaluation across all DHS Components to instruct on how to determine their current maturity and compliance levels. The DHS self-evaluation method considered the maturity levels as cumulative capabilities in terms of reporting to OMB. Specifically, the EL tiers, described in the table below, are classified by rating categories which enables Components to prioritize their efforts and resources so that, over time, Components achieve full compliance with requirements for implementation.

Further, using the EL tier classifications as part of the self-evaluation process allows Components to identify resource requirements to fill gaps in their EL maturity levels. Components identify the need for additional monitoring tools to track potentially malicious activities, including data storage for log retention and analytic software licenses. In the October 26, 2021 report to OMB, pursuant to M-21-31, DHS identified resources needed in order to fully meet EL1, EL2, and EL3. Since the resources required for EL1 represent a foundational investment for building the required capabilities defined in EL2 and EL3, DHS is not yet able to determine a timeline for EL-2 and EL-3.

Summary of Event Logging Tiers from M-21-31, August 27, 2021

EL Tiers	Rating	Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

DHS OCIO will continue discussions with OMB concerning resources and implementation guidance. DHS OCIO will also continue generating quarterly reports for Component visibility and assist with guidance on implementation and improvements. ECD: To Be Determined.

4

Appendix VII: Comments from the Department of the Interior

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Edward Alexander, Jr.
Assistant Director, Information Technology
and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks and Mr. Alexander:

Thank you for providing the U.S. Department of the Interior (Department, Interior) the opportunity to review and comment on the draft Government Accountability Office (GAO) report titled, *CYBERSECURITY: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements* (GAO-24-105658). We appreciate GAO's review of the Department's Cybersecurity Program.

The GAO issued several recommendations to multiple agencies, including one to Interior to address its finding. The Department concurs with the recommendation. Below is a summary of actions planned to implement the recommendation.

Recommendation 8: The Secretary of the Interior should ensure that the Department of the Interior fully implements all event logging requirements as directed by OMB guidance.

Response: Concur. Interior requested funding in the 2024 President's Budget to implement event logging capabilities to achieve tier EL-1 of the OMB guidance. Assuming Congress enacts the President's Budget request, the Department will implement the planned solution to achieve tier EL-1. The Department will continue to work with OMB and update its internal guidance to facilitate implementation, taking a prioritized approach to both the devices logged and the maturity model elements.

If you have any questions or need additional information, please contact Darren B. Ash, Chief Information Officer, at Darren_Ash@ios.doi.gov.

Sincerely,

JOAN MOONEY

Digitally signed by JOAN MOONEY
Date: 2023.11.07 16:33:58 -05'00'

Joan M. Mooney
Principal Deputy Assistant Secretary
Exercising the Delegated Authority of the Assistant Secretary- Policy, Management and Budget

Appendix VIII: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

November 8, 2023

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report, ***Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements*** (GAO-24-105658).

The enclosure contains the actions to be taken to address the draft report recommendation. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Kimberly Jackson
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs Comments to
Government Accountability Office Draft Report
Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements
(GAO-24-105658)

Recommendation 14: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully implements all event logging requirements as directed by OMB guidance.

VA Response: Concur. The Department of Veterans Affairs (VA) agrees with the Government Accountability Office's (GAO) conclusions and concurs with its recommendation to the Department. VA is compliant with two of the three primary incident response requirements from Executive Order 14028, Improving the Nation's Cybersecurity. VA has prioritized efforts to comply with the third requirement to assess event logging maturity against the maturity model in Office of Management and Budget Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, to identify gaps associated with completing each of the requirements and to reach event logging tier 3. VA is working to ensure the logging of system events and telemetry, specifically, for VA's most critical systems, in accordance with M-21-31 and the Cybersecurity and Infrastructure Security Agency's December 2022 implementation guidance.

Target implementation date: September 30, 2024, for VA critical systems.

Appendix IX: Comments from the Environmental Protection Agency

OFFICE OF MISSION SUPPORT
WASHINGTON, D.C. 20460

November 13, 2023

Ms. Jennifer Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. Franks,

Thank you for the opportunity to review and comment on GAO's draft report, "Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements" (GAO-24-105658).

The purpose of this letter is to provide the U.S. Environmental Protection Agency's response to your recommendation. The Agency agrees with the GAO's findings, conclusions, and recommendations related to the EPA.

In general, GAO found that 20 agencies have not met the requirements for investigation and remediation (event logging) capabilities. Office of Management and Budget (OMB) requires agencies to reach the advanced tier 3, which means all logging requirements at all criticality levels are met. EPA has made considerable progress in achieving the logging requirements and has an ongoing project to implement all logging requirements in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities*.

GAO Recommendation:

The Administrator of the Environmental Protection Agency should ensure that the Agency fully implements all event logging requirements as directed by OMB guidance. (Recommendation 15)

EPA Response:

The EPA agrees with this finding and recommendation. The Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) is collaborating with Agency Regions and Program Offices to fully implement all event logging requirements as outlined in OMB M-21-31. The Agency will continue the ongoing project to implement all event logging requirements and estimates this will be completed by August 15, 2024.

In closing, the EPA agrees with the findings and recommendation from the GAO report. Again, thank you for the opportunity to review the draft report. If there are any questions, please contact Afreeka Wilson at Wilson.Afreeka@epa.gov, (202) 564-0867 (Desk).

Sincerely,

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.11.13 08:54:47 -05'00'

Vaughn Noga
Chief Information Officer

cc:
Jennifer R. Franks FranksJ@gao.gov
Edward Alexander, Jr. AlexanderE@gao.gov
Season Burris BurrisS@gao.gov
Cyber IR CyberIR@gao.gov
Vaughn Noga
David Alvarado
Austin Henderson
Tonya Manning
Mark Bacharach
Lee Kelly
Kaitlyn Khan
Daniel Coogan
Yulia Kalikhman
Janice Jablonski
Marilyn Armstrong
Afreeka Wilson
OMS_Audit_Coordination
EPA GAO Liaison Team
Susan Perkins

2

Appendix X: Comments from the General Services Administration

DocuSign Envelope ID: 905BA209-1AFE-4D94-8E4A-E1C34F7AA949

GSA

The Administrator

November 16, 2023

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Comptroller General:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) Draft Report - *Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements* (GAO-24-105658).

GAO made the following recommendation to GSA:

> 016: The Administrator of the General Services Administration should ensure that the General Services Administration fully implements all event logging requirements as directed by OMB guidance.

GSA agrees with the recommendation and is developing a plan to take appropriate action. If you have any questions or concerns, please contact me or Gianelle Rivera, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

Robin Carnahan
Administrator

cc: Jennifer R. Franks, Director, Information Technology and Cybersecurity, GAO

U.S. General Services Administration
1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

Appendix XI: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001

Reply to Attn of: Office of Chief Information Officer

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Franks:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements" (GAO-24-105658), dated October 11, 2023.

GAO determined that many Chief Financial Officer (CFO) Act agencies have made progress in incident response preparedness by taking steps to standardize their incident response plans and demonstrating improvement in their capabilities for incident detection analysis. However, many agencies have not met requirements for investigation and remediation (event logging) capabilities.

In the draft memorandum, GAO makes one recommendation addressed to the NASA Administrator.

Specifically, GAO recommends the following:

Recommendation 1: The Administrator of the National Aeronautics and Space Administration should ensure that the agency fully implements all event logging requirements as directed by OMB guidance.

Management's Response: NASA concurs with this recommendation.

NASA has had several challenges given the specialized and intricate nature of NASA's operations and the comprehensive breadth of M-21-31:

- Scope of M-21-31: The wide-ranging requirements of M-21-31 is daunting when combined with NASA's already complex Information Technology (IT) ecosystem.
- Complexity in Data Integration: The multifaceted nature of NASA's systems, some of which are uniquely designed for space missions, poses inherent challenges to integration.

- Resource Constraints: Budgetary and human resource limitations impede progress towards realizing NASA's future state logging solution while continuing to operate and maintain the existing enterprise logging solution.

Despite these challenges, NASA's Office of the Chief Information Officer (OCIO) has established a Cybersecurity Improvement Portfolio (CIP) and is leading efforts to create a comprehensive plan addressing all three Event Logging (EL) tiers for all systems. A statement of work has been developed, which includes several key requirements. Within 210 days of contract issuance, the statement of work mandates the delivery of two specific outcomes:

- Enterprise Cyber Logging Strategic Plan: The development of a strategic plan outlining NASA's approach to achieving Event Logging Tier 3 compliance. This plan will also address all other investigative and remediation requirements as specified by Federal mandates.
- Action Plan: A detailed action plan with project management-level implementation details for executing the Enterprise Cyber Logging strategic plan. This action plan will provide a roadmap for how NASA intends to implement the strategic goals outlined in the cybersecurity logging plan.

These deliverables are crucial components of NASA's plan to achieve EL3 and align with Federal mandates.

Estimated Completion Date: January 31, 2025.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Matthew Degrave at (757) 864-6838.

Sincerely,

Leigh anne Giraldi Digitally signed by Leigh anne Giraldi Date: 2023.11.06 17:52:45 -05'00'

Jeff Seaton
Chief Information Officer
Office of the Chief Information

Appendix XII: Comments from the Nuclear Regulatory Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 6, 2023

Jennifer R. Franks, Director,
Center for Enhanced Cybersecurity
Information Technology and
Cybersecurity
U. S. Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Director Franks:

Thank you for giving the U.S. Nuclear Regulatory Commission (NRC) the opportunity to review and comment on the U.S. Government Accountability Office's draft report GAO-24-105658, "Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements." The NRC has reviewed the draft report, is in general agreement with it, and does not have any comments.

Sincerely,

Daniel H. Dorman

Digitally signed by Daniel H. Dorman
Date: 2023.11.06 11:41:49 -05'00'

Daniel H. Dorman
Executive Director
for Operations

Appendix XIII: Comments from the Office of Personnel Management

Office of the
Chief Information
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

November 9, 2023

Mr. Edward Alexander, Jr.
Assistant Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Alexander:

Thank you for the opportunity to respond to the U.S. Government Accountability Office (GAO) draft report, Cybersecurity – Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements, GAO-24-105658.

Our responses to your recommendations are below.

Recommendation #19: The Director of the Office of Personnel Management should ensure that the agency fully implements all event logging requirements as directed by OMB guidance.

Management Response: Concur. OPM acknowledges the importance of logging events to identify and investigate cybersecurity threats against the agency. OPM is logging several events. OPM is prioritizing projects and initiatives with the goal of identifying and investigating cybersecurity threats against the agency by logging all cyber events, despite limited available resources including funding.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mark W. Lambert, (202) 606-2980, or Mark.Lambert@opm.gov.

Sincerely,

GUY CAVALLO
Digitally signed by GUY CAVALLO
Date: 2023.11.09 16:38:55 -05'00'

Guy Cavallo
Chief Information Officer
U.S. Office of Personnel Management

OPM.GOV Empowering Excellence in Government through Great People USAJOBS.GOV

Appendix XIV: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

November 9, 2023

Jennifer R. Franks
Director of Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Franks,

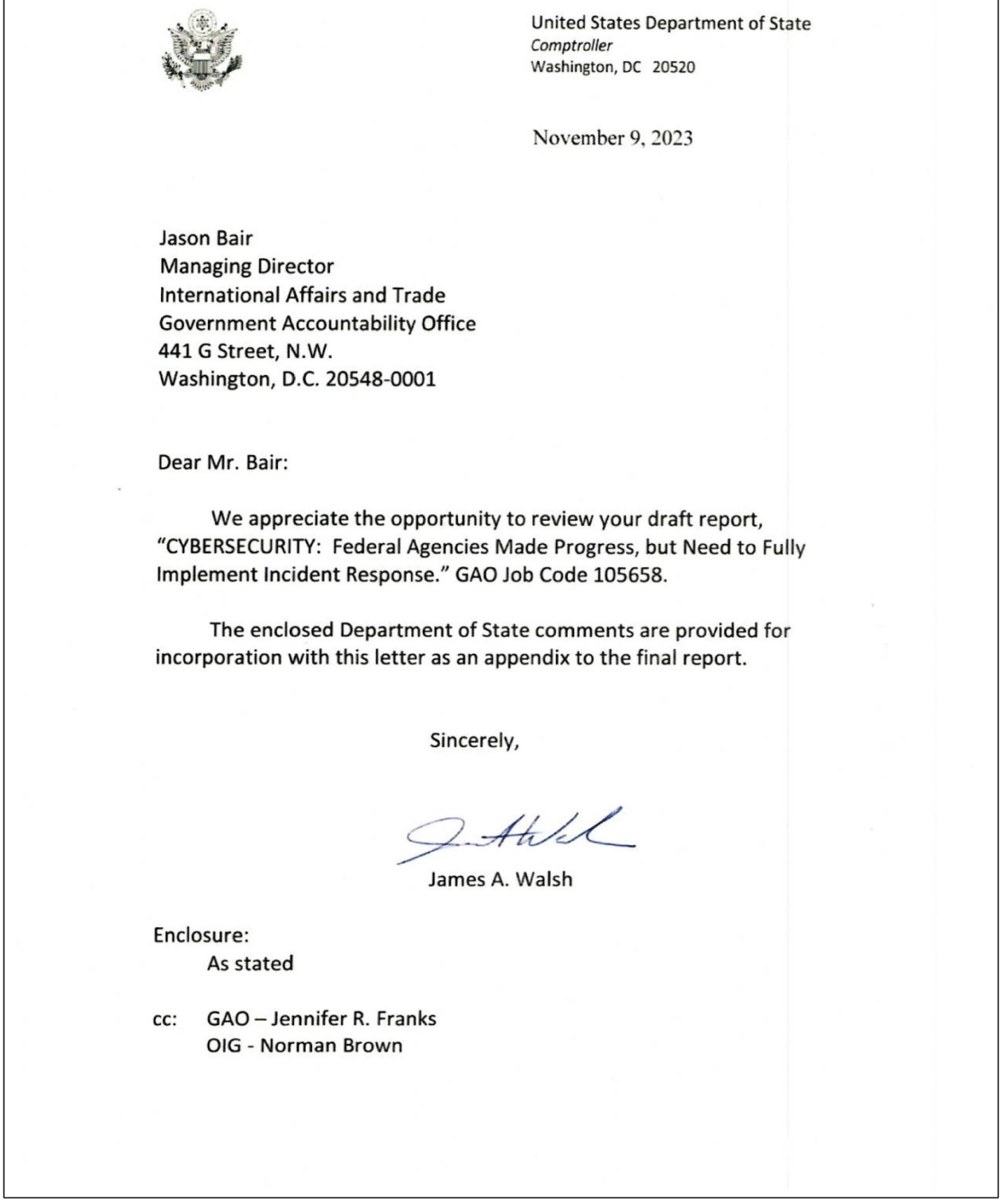
Thank you for the opportunity to review the Draft Report, "Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements" (GAO-24-105658). We agree with the recommendation.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Scott Frey
Chief of Staff

Appendix XV: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

November 9, 2023

Jason Bair
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Bair:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: Federal Agencies Made Progress, but Need to Fully Implement Incident Response." GAO Job Code 105658.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

James A. Walsh

Enclosure:
As stated

cc: GAO – Jennifer R. Franks
OIG - Norman Brown

Department of State Response to Draft Report Request

CYBERSECURITY: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements
(GAO-24-105658, GAO Code 105658)

Thank you for the opportunity to comment on the draft report, *Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response*.

Recommendation: The Secretary of State should ensure that the Department of State fully implements all event logging requirements as directed by OMB guidance. (Recommendation 11)

Response: The Department of State continues its progress in achieving event logging compliance as directed by OMB. As such, State has published a system standard document for logging "Audit Log Sharing Security Standard (AL3S)." This document serves as a mandatory requirement for system owners to ensure their FISMA systems are configured to log all events identified in OMB Memorandum M-21-31. Additionally, State coordinates with stakeholders to include system owners, technical experts, project managers, and senior leadership under "Project Lakehouse." This effort involves the design and implementation of an enterprise service that enables processing, collection, and storage of data elements in compliance with M-21-31. State acknowledges this gap and continues its compliance improvement and increasing the number of systems, with a priority on High Value Assets (HVAs) through the Lakehouse Project. While we anticipate improvements in M-21-31 systems adherence in the next fiscal year, this effort will require a multi-year approach and continual attention.

Appendix XVI: Comments from the United States Agency for International Development

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

November 7, 2023

Re: CYBERSECURITY: FEDERAL AGENCIES MADE PROGRESS, BUT NEED TO FULLY IMPLEMENT INCIDENT RESPONSE REQUIREMENTS (GAO-24-105658)

Dear Ms. Franks:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements (GAO-24-105658).

USAID is committed to continuously improving our investigative and remediation capabilities related to cybersecurity incidents as federally mandated by OMB M-21-31. USAID M/CIO continues to perform due diligence in capturing all OMB M-21-31 compliance requirements through careful vendor selection while executing continuous improvement of log ingestion in a reasonable and prudent manner. In addition, we issued a contract dedicated to this effort in October 2022 and have made significant progress with its implementation.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our incident response program.

Sincerely,

Colleen R Allen

Colleen Allen
Assistant Administrator
Bureau for Management

Enclosure: a/s

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON THE DRAFT REPORT PRODUCED BY THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) TITLED, Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements (GAO-24-105658)

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team, and the specific findings that will help USAID achieve greater effectiveness in our incident response program.

The draft report contains one recommendation for USAID:

The Administrator of the U.S. Agency for International Development Should ensure that the agency fully implements all event logging requirements as directed by OMB guidance.

The issue cited in this recommendation has already been addressed to USAID M/CIO in a separate audit report: *The USAID Office of the Inspector General (OIG) A-000-23-004-C Federal Information Security Management Act (FISMA) Audit Report*, issued 9/8/2023.

That report's recommendation states:

> **[USAID should] Fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.**

The corresponding management comments and target completion date provided to OIG are as follows:

> Management Comments: M/CIO agrees with the recommendation. M/CIO will fully implement event logging (EL) requirements in accordance with Office of Management and Budget, Memorandum M-21-31 with the top focus being an overall improved security posture.
>
> Target Completion Date: December 31, 2023.

USAID notified GAO of this by electronic mail on October 18, 2023. GAO responded per electronic mail on October 19, 2023 that GAO will thus remove the recommendation to USAID from the final audit report for Engagement GAO-24-105658. This communication is being provided as documentation to support this Management Comments response.

Appendix XVII: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the individual named above, Edward Alexander, Jr. (Assistant Director), Season Burris (Analyst in Charge), Christopher Businsky, Linda Erickson, Rebecca Eyler, Katherine Fetrow, Camille Garcia, Julia Munroe, Scott Pettis, Elizabeth Simonelli, Umesh Thakkar, and Curt Williams made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548