Federal Cybersecurity Incident Response Capabilities

(GAO-24-105658)

Jennifer Franks, Director

Center for Enhanced Cybersecurity

March 21, 2024

```
erver sshd[8016]: Failed password for root
erver sshd[8189]: Failed password for root f
shd[8189]: last message repeated 2 times
rver sshd[8194]: Failed password for root f
ver sshd[8194]: Failed password for root f
ver sshd[8304]: Failed password for root f
hd[8304]: last message repeated 2 times
er sshd[8309]: Failed password for root fr
er sshd[8309]: Failed password for root fr
sshd[8547]: Failed password for root fr
sshd[8553]:
```

Source: 123tin/stock.adobe.com.

GAO’s Mission

GAO exists to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people.

We provide Congress with timely information that is objective, fact-based, nonpartisan and non-ideological.

Cyber Risks Impact Everyone!

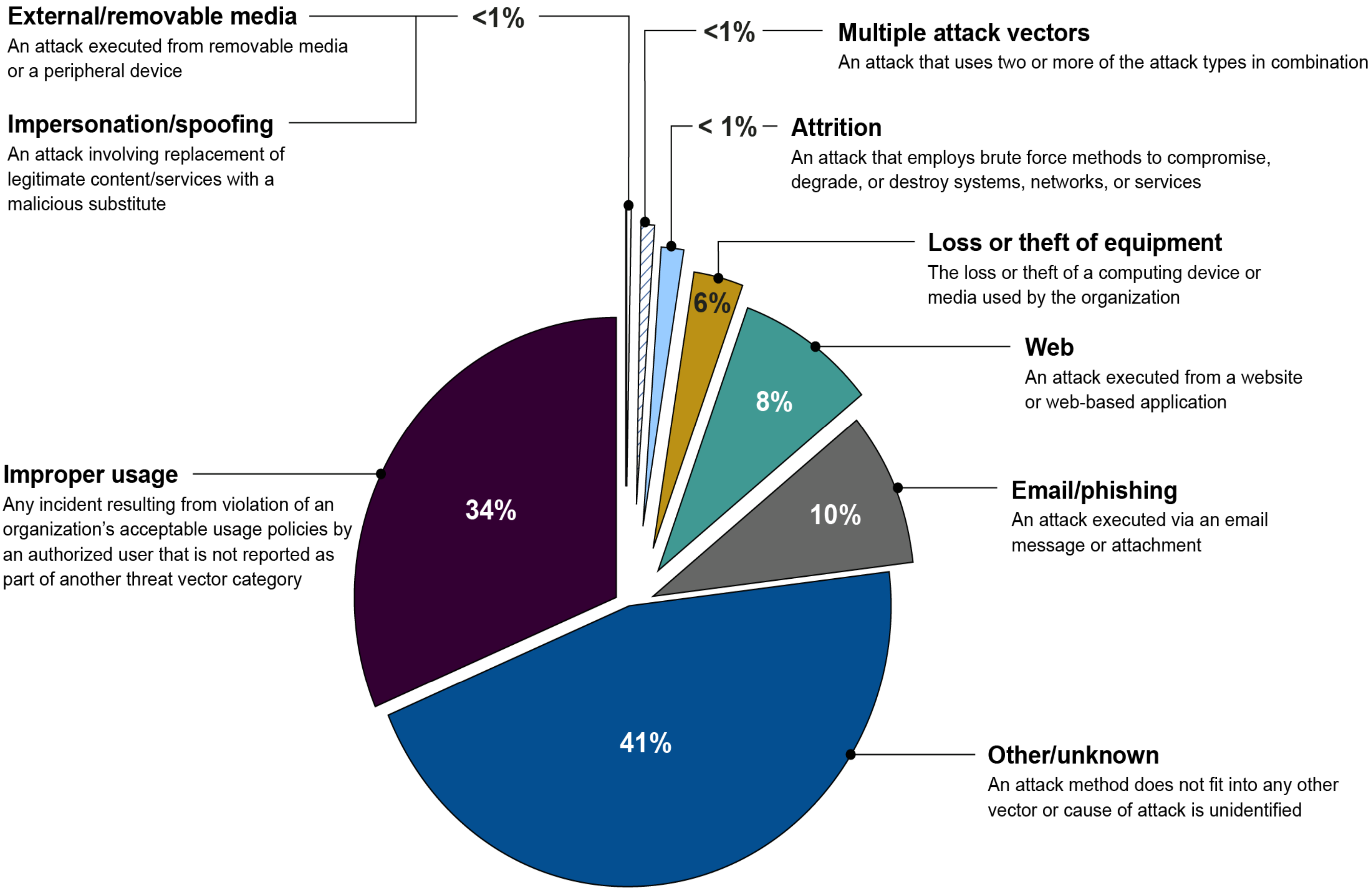
- Federal agencies and our nation’s critical infrastructure—such as energy, transportation systems, communications, and financial services—depend on IT systems to carry out operations and process essential data.

- Risks to these IT systems are increasing—including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks.

- **Over 30,000** security incidents were reported by federal civilian agencies to the Department of Homeland Security in **FY 2022**.

https://www.gao.gov/cybersecurity

Federal agencies reported 30,659 information security incidents in fiscal year 2022



External/removable media
An attack executed from removable media or a peripheral device

Impersonation/spoofing
An attack involving replacement of legitimate content/services with a malicious substitute

Multiple attack vectors
An attack that uses two or more of the attack types in combination

Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

Web
An attack executed from a website or web-based application

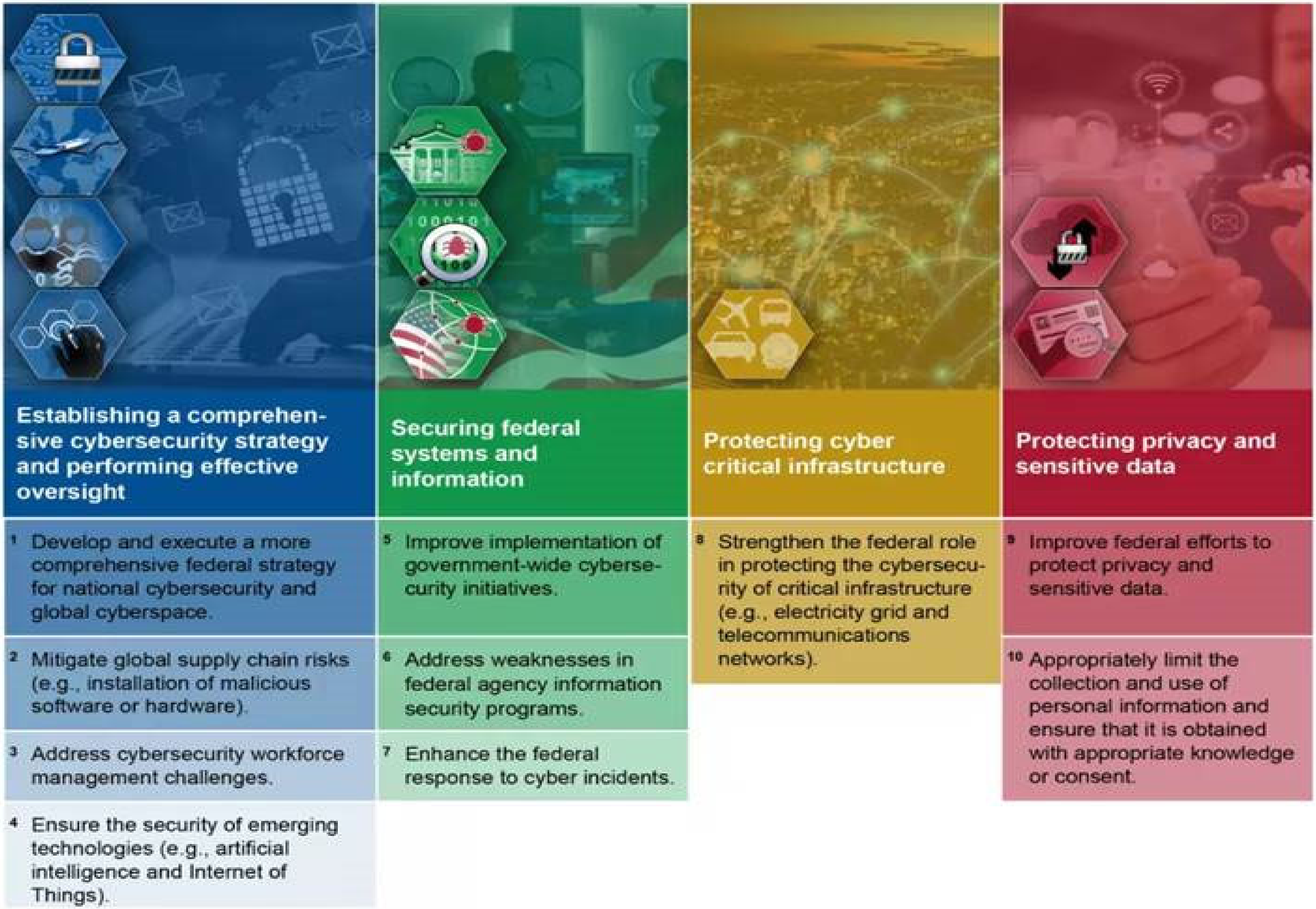
Email/phishing
An attack executed via an email message or attachment

Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

Other/unknown
An attack method does not fit into any other vector or cause of attack is unidentified

Source: United States Computer Emergency Readiness Team incident report data for fiscal year 2022.

GAO Cybersecurity High-Risk List 2023



Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis.

CEC History

The **Center for Enhanced Cybersecurity (CEC),** formerly known as the GAO e*Security Lab, has been in existence testing, evaluating, and reporting on federal information security for over 25 years.

Since that time, GAO has listed cybersecurity on its high-risk list and credits this designation as the impetus for initially developing this in-house technical evaluation capability.

With rapidly evolving threats and vulnerabilities escalating from around the globe, the attention to cybersecurity has continued to increased.

CEC Leads in Cybersecurity Recommendations Made to Federal Agencies

Since 2010, GAO made more than 4,200 recommendations to agencies aimed at addressing cybersecurity challenges facing the government.

Of these, the CEC has led the development of about 50% of the cybersecurity recommendations. We identified weaknesses in key safeguards to limit, prevent, and detect inappropriate access to computer resources and maintain secure configurations of software and hardware.

More than 130 of these recommendations were made since the last high-risk update in 2023. As of March 1, 2024, about 900 recommendations had not been fully implemented, including 64 of 162 priority recommendations, which we believe warrant priority attention from heads of key departments and agencies.

Federal Incident Report Objectives
(GAO-24-105658)

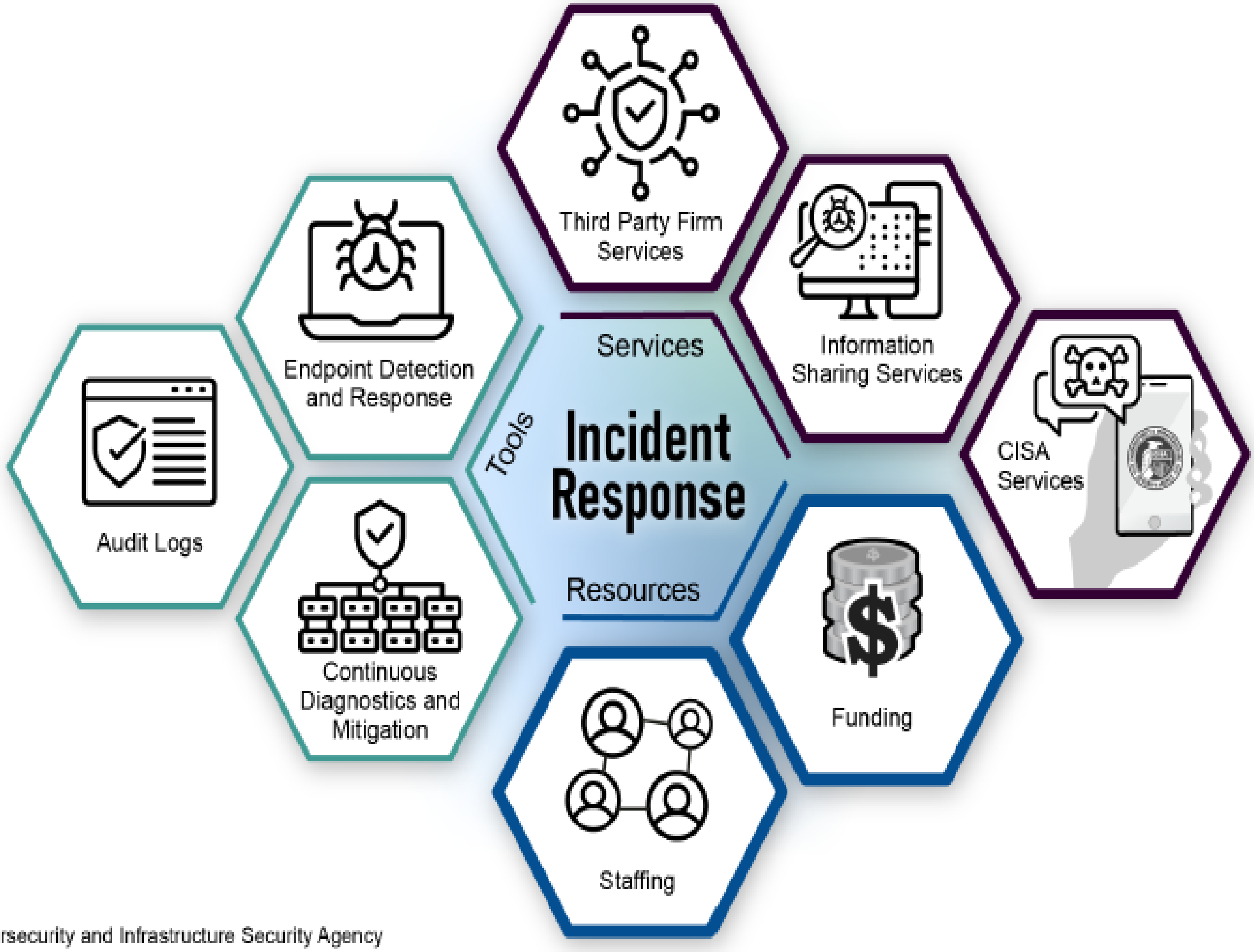
- Describe the capabilities agencies use to prepare for and respond to cybersecurity incidents,
- Evaluate the extent to which agencies have made progress in preparing for cybersecurity incident response, and
- Describe the challenges agencies face in preparing for incident response and the efforts to address them.

Objective 1: Agencies Rely Upon Tools, Services, and Resources for Incident Response

Specifically, they depend on:

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

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


Incident Response
Tools
Services
Resources
Third Party Firm Services
Information Sharing Services
CISA Services
Endpoint Detection and Response
Audit Logs
Continuous Diagnostics and Mitigation
Funding
Staffing

CISA = Cybersecurity and Infrastructure Security Agency

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

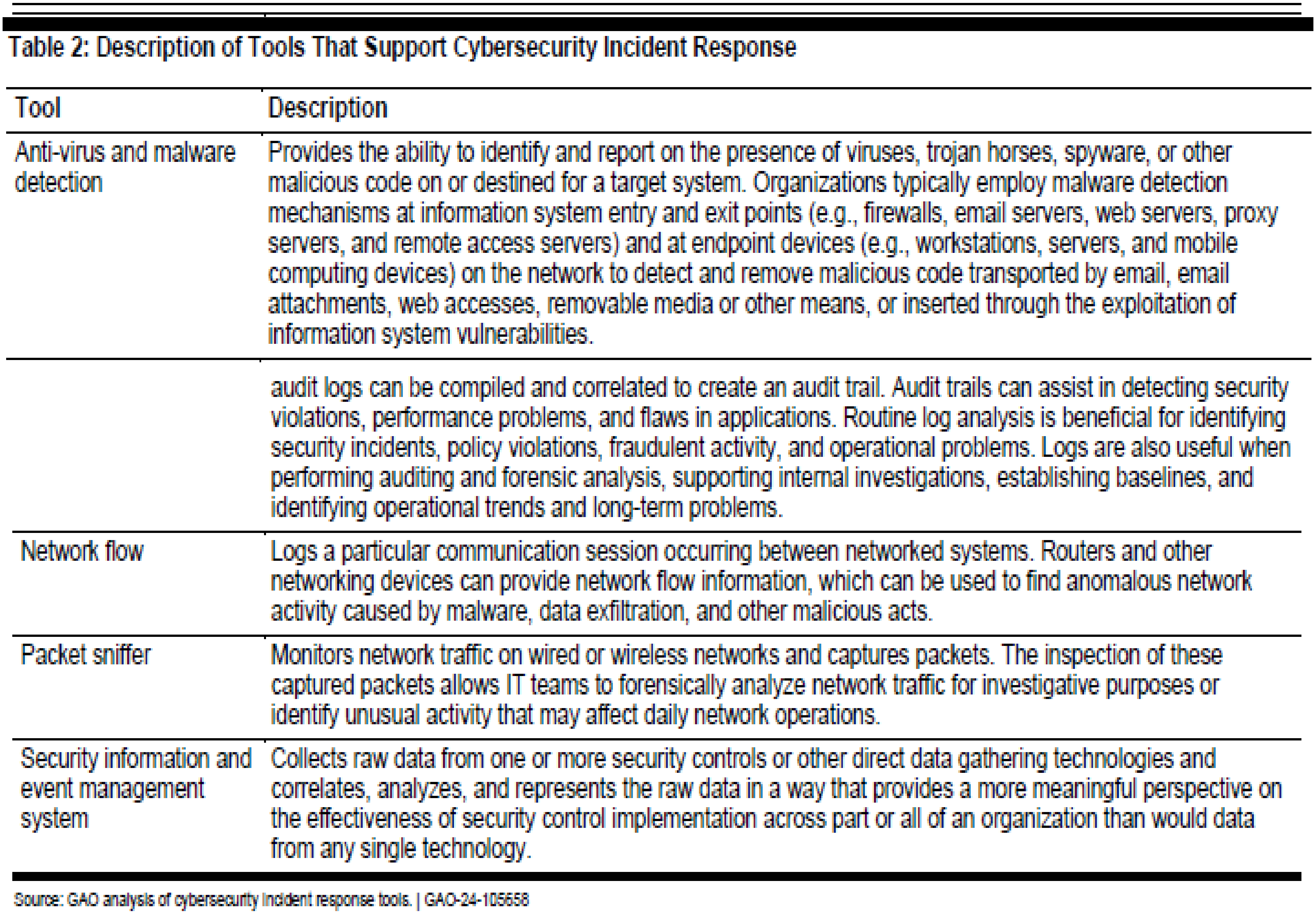


Table 2: Description of Tools That Support Cybersecurity Incident Response

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.
	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

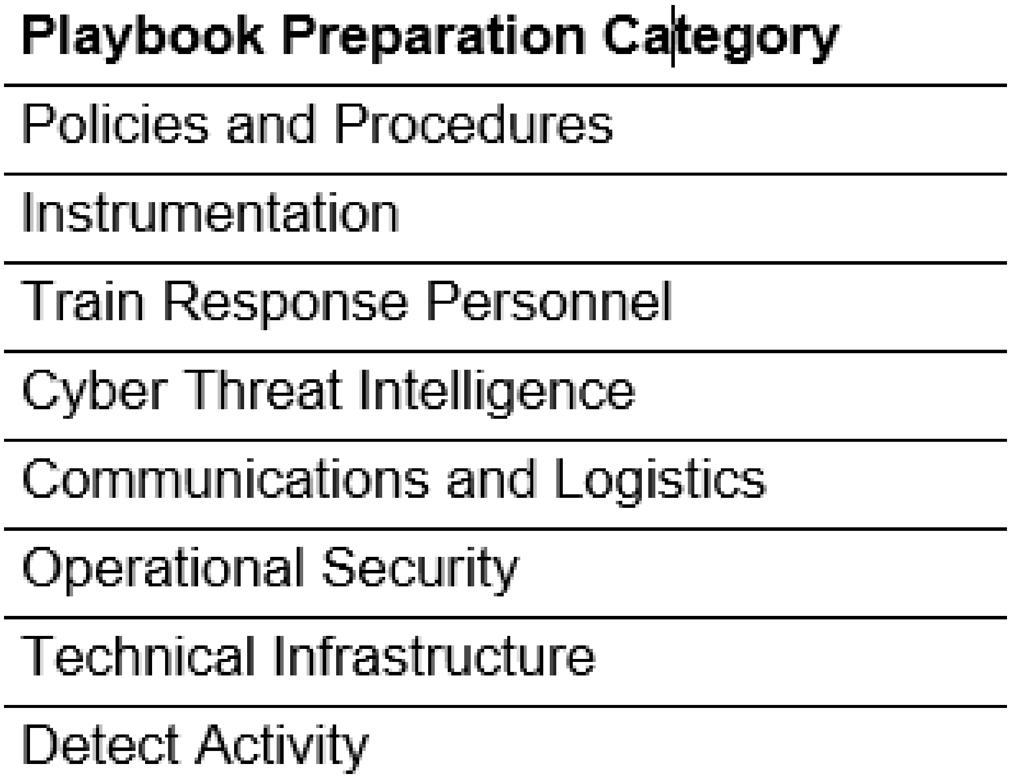
Objective 2: Agencies Made Progress in Certain Incident Response Areas, but Have Not Met Event Logging Requirements

- The 23 CFO Act agencies have made progress in cybersecurity incident response preparedness.

- 20 agencies have not met requirements for investigation and remediation capabilities.

Agencies Are Taking Steps to Standardize Incident Response Plans and Processes

- All 23 agencies that we assessed demonstrated that they substantially completed the playbook's incident response preparation activities.



Playbook Preparation Category
Policies and Procedures
Instrumentation
Train Response Personnel
Cyber Threat Intelligence
Communications and Logistics
Operational Security
Technical Infrastructure
Detect Activity

Agencies Have Made Progress in Incident Detection

- **Continuous Diagnostic & Mitigation (CDM):** all 23 agencies have signed a CDM MOA

- **Endpoint Detection & Response (EDR):** 23 agencies have identified a tool and are working to implement.

Most Agencies Have Not Met Event Logging Capability Requirements

- OMB’s August 2021 memorandum
- Information from logs can provide valuable insight

As of August 2023, 17 agencies were at tier 0, and three agencies were at tier 1. Officials stated their agencies were **not expected to meet the tiers soon**.

Event Logging Implementation

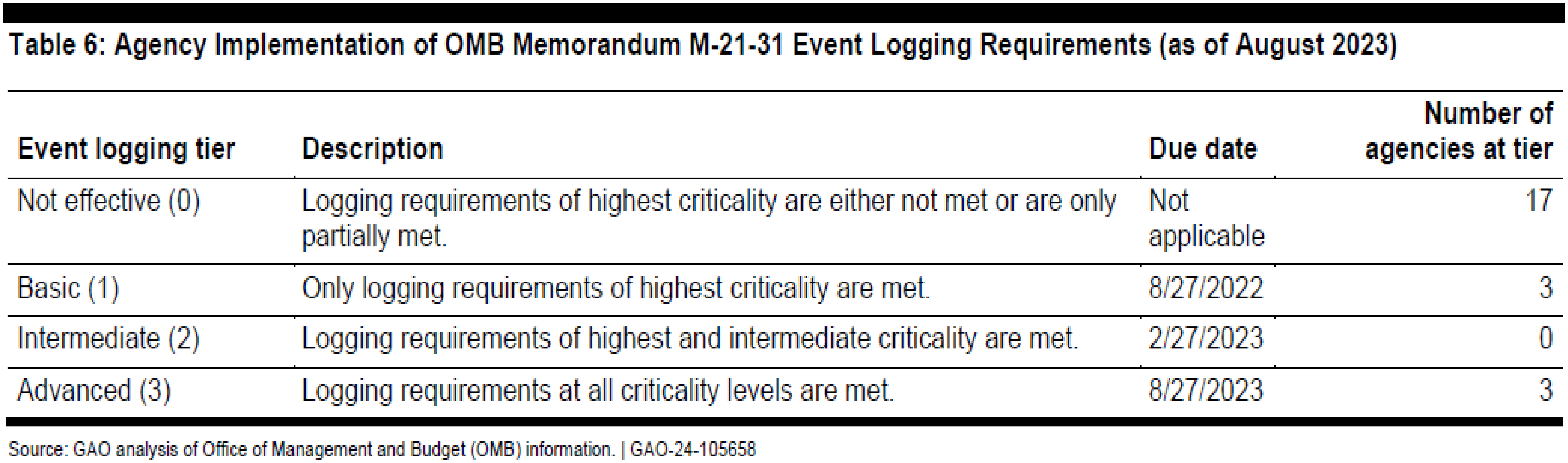


Table 6: Agency Implementation of OMB Memorandum M-21-31 Event Logging Requirements (as of August 2023)

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

Three Agencies Met Tier 3

- **Tier 3:**
  - Department of Agriculture,
  - National Science Foundation,
  - Small Business Administration
- Officials from SBA and USDA credited their agencies' successes to agency efforts that preceded the issuance of the OMB memorandum.

Objective 3: 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 be fully prepared to respond to cybersecurity incidents:

  1. lack of staff;
  2. technical challenges in event logging; and
  3. limitations in cyber threat information sharing.

- Federal entities have initiated efforts that can assist in overcoming these challenges.

Challenge 1: Lack of Staff

- 16 of 24 agencies reported **needing additional staff or positions to carry out incident response activities**.
  - Areas include: intelligence, threat, and forensic analysts, as well as hunt teams.
  - Six agencies also mentioned having unfilled positions within the security operations center (SOC), including SOC leads, analysts, and supervisors.
- Eight of 23 agencies cited **staffing as a gap or challenge in meeting event logging requirements** established in OMB M-21-31.
  - One official stated that it would need to triple the size of the current team responsible to ensure compliance with certain federal requirements in the memo

Challenge 2:
Technical Challenges in Event Logging

- 20 of the 23 agencies had not met the tiered event logging requirements established by OMB.
- Technical challenges agencies reported included:
  - 12 agencies reported **gaps in technology or complexities within existing technical environments** (e.g., legacy systems) proved challenging in meeting the requirements.
  - 17 agencies reported the **need for increased storage capacity** to meet event logging requirements.
    - Increase storage capacity for logs needed to meet event logging levels.
    - One agency would need to expand logging from 7 terabytes of log data (with retention of 1 year) to 70 terabytes per day.
    - Another stated they already collect over 13 billion logs daily, accounting for almost 15 terabytes of data per day.

Challenge 3:
Limitations in Cyber Threat Information Sharing

- 14 of the 24 agencies reported **classification challenges** in collecting, aggregating and sharing cyber threat intelligence data.
  - Taking an indicator of compromise from a classified network to use on an unclassified network.
  - Not having enough cleared staff to access and analyze classified data.
- 13 agencies reported challenges with the **quality or the timeliness** of the data being shared.
  - Nine agencies stated that they receive such large volumes of cyber threat intelligence from a variety of sources resulting in **redundant or out-of-date information**

Federal Efforts Underway

- **Ongoing federal efforts include:**
  - on-site cyber incident response assistance from CISA,
  - event logging workshops and guidance,
  - enhancements to a cyber threat information sharing platform.
- **Longer-term efforts include:**
  - implementation of the National Workforce and Education Strategy
  - a new threat intelligence platform offering from CISA, targeted to roll out its first phase to federal departments and agencies in fiscal year 2024.

Recommendations

- We made recommendations to the heads of 19 agencies to fully implement event logging requirements.[1]
  - Sixteen agencies agreed with the recommendations and three neither agreed nor disagreed.
- We also made a recommendation to the Director of CISA to 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.

[1] While we initially had a recommendation to USAID in the draft report, during the agency 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. Therefore, we removed the recommendation to USAID.

Questions/Answers

Jennifer R. Franks

Director, Center for Enhanced Cybersecurity

FranksJ@gao.gov

GAO on the Web

Web site: http://www.gao.gov/

Congressional Relations

Orice Williams Brown, Managing Director, williamso@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

Copyright