



April 2024

CYBERSECURITY Implementation of Executive Order Requirements Is Essential to Address Key Actions

Accessible Version

GAO Highlights

View [GAO-24-106343](#). For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcaim@gao.gov.

Highlights of [GAO-24-106343](#), a report to congressional committees

April 2024

CYBERSECURITY

Implementation of Executive Order Requirements Is Essential to Address Key Actions

Why GAO Did This Study

For more than 25 years, GAO has identified information security as a high-risk area. During this period, the threat of cyber-based attacks on IT systems has continued to grow. In 2021, the President issued Executive Order 14028 to enhance federal resilience in protecting IT systems. The order contains requirements for federal agencies to improve their ability to identify, protect against, and respond to malicious cyber threats.

The Federal Information Security Modernization Act of 2014 includes a provision for GAO to periodically report on agencies' progress in improving their cybersecurity practices. This report examines the extent to which (1) agencies have implemented Executive Order 14028 leadership and oversight-related requirements and (2) the order has addressed federal cybersecurity challenges.

To do so, GAO identified government-wide leadership and oversight requirements in the order and the key agencies required to perform them. GAO then reviewed the agencies' implementation of those requirements. GAO also compared challenges identified in its work and in discussions with federal CISOs against the content of the order to determine whether they were addressed.

What GAO Recommends

GAO is making two recommendations to DHS and three to OMB to fully implement the order's requirements. DHS agreed with recommendations to further define critical software and improve operations of the Cyber Safety Review Board. OMB stated it had no comments on GAO's report.

What GAO Found

Among its 115 provisions, the order contains 55 leadership and oversight requirements (actions to assist or direct the federal agencies in implementing the order). The three key agencies primarily responsible for the implementation of these requirements are the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Technology, and the Office of Management and Budget (OMB). These agencies fully completed 49 of the 55 requirements, partially completed five, and one was not applicable (see

table below). Completing these requirements would provide the federal government with greater assurance that its systems and data are adequately protected.

Progress in Implementing Executive Order 14028 Leadership and Oversight Requirements, as of March 2024

Executive Order Section	Number of requirements that are:			
	Fully complete	Partially complete	Not complete	Not applicable
Removing Barriers to Sharing Threat Information	6	1	no requirements received this score	no requirements received this score
Modernizing Federal Government Cybersecurity	8	no requirements received this score	no requirements received this score	no requirements received this score
Enhancing Software Supply Chain Security	16	1	no requirements received this score	no requirements received this score
Establishing a Cyber Safety Review Board	6	1	no requirements received this score	no requirements received this score
Standardizing Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	4	no requirements received this score	no requirements received this score	1
Improving Detection of Cybersecurity Vulnerabilities and Incidents	7	1	no requirements received this score	no requirements received this score
Improving the Federal Government's Investigative and Remediation Capabilities	2	1	no requirements received this score	no requirements received this score
Total	49	5	no requirements received this score	1

Legend: fully complete = those where the actions required are complete; partially complete = those where GAO judged significant, but not complete, progress to be made in completing a requirement; not complete = those where the progress made toward completion was minimal and not significant. The symbol “—” indicates that no requirements received this score.

Source: GAO analysis of documentation from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency; the National Institute of Standards and Technology; and the Office of Management and Budget. | GAO-24-106343

GAO’s High-Risk Series identified ten action areas critical to addressing the nation’s cybersecurity challenges. The order’s requirements directly address five of these ten critical action areas, while each of the other five could be addressed by other recently-issued strategies, frameworks, and guidance. For example, the cyber workforce and critical infrastructure action areas could potentially be addressed by the *National Cyber Workforce Strategy* and *National Cybersecurity Strategy*, if implemented effectively. In addition to the ten action areas, six federal chief information security officers (CISO) identified additional cyber issue areas they considered to be challenging, such as uncertainty in cyber funding, creating a culture that prioritizes cybersecurity as an essential mission component, and focus on cyber compliance versus cyber resilience. The order’s requirements also address each of these additional cyber issue areas identified by CISOs. For example,

the order addresses uncertainties in cyber funding by requiring OMB to assist agencies in having sufficient resources to implement its requirements.

Contents

GAO Highlights	ii
Why GAO Did This Study	ii
What GAO Recommends	ii
What GAO Found	ii
<hr/>	
Letter	1
Background	4
Agencies Implemented Most of the Order’s Leadership and Oversight Requirements	14
Existing Guidance Expected to Assist Agencies in Addressing Cybersecurity Challenges	34
Conclusions	42
Recommendations for Executive Action	43
Agency Comments and Our Evaluation	43
<hr/>	
Appendix I: Objectives, Scope, and Methodology	46
Appendix II: Responsibilities in Executive Order 14028	49
Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028	59
Appendix IV: Comments from the Department of Homeland Security	68
Appendix V: GAO Contacts and Staff Acknowledgments	76
<hr/>	
Tables	
Progress in Implementing Executive Order 14028 Leadership and Oversight Requirements, as of March 2024	iii
Table 1: Number and Types of Responsibilities Assigned for Actions in Executive Order 14028	12
Table 2: Progress in Implementing Executive Order 14028 Leadership and Oversight Requirements, as of March 2024	15
Table 3: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Removing Barriers to Threat Information, as of March 2024	16

Table 4: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Modernizing Federal Government Cybersecurity, as of March 2024	19
Table 5: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Enhancing Software Supply Chain Security, as of March 2024	20
Table 6: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Establishing a Cyber Safety Review Board, as of March 2024	24
Table 7: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Standardizing the Federal Government’s Playbook, as of March 2024	27
Table 8: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks, as of March 2024	29
Table 9: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Improving the Federal Government’s Investigative and Remediation Capabilities, as of March 2024	31
Table 10: Provisions and Agencies Responsible in Executive Order 14028	49
Table 11: Status and Details of Leadership and Oversight Requirements in Executive Order 14028, as of March 2024	59

Figures

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions	5
Figure 2: Overview of Executive Order 14028 Sections	10
Figure 3: GAO’s 10 High-Risk Critical Action Areas Addressed by Executive Order 14028 (EO)	36

Abbreviations

CDM	continuous diagnostics and mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CISO	chief information security officer
DHS	Department of Homeland Security
DOD	Department of Defense

EDR	endpoint detection and response
FCEB	Federal Civilian Executive Branch
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IT	information technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
SBOM	Software Bill of Materials
ZTA	zero trust architecture

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



April 18, 2024

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

Federal IT systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. The complexity of these systems increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising federal systems and networks. The IT systems supporting federal agencies are inherently at risk.

Safeguarding federal computer systems has been a longstanding concern. More than 25 years have passed since GAO's first designation in 1997 of information security as a government-wide high-risk area. We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003.¹ We added protecting the privacy of personally identifiable information in 2015 and establishing a comprehensive cybersecurity strategy and performing effective oversight in 2018.² Most recently, we continued to identify

¹See GAO, *High-Risk Series: An Overview*, [GAO/HR-97-1](#) (Washington, D.C.: Feb. 1, 1997) and *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 1, 2003).

²GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: Sept. 6, 2018) and *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

federal information security as a government-wide high-risk area in our April 2023 high-risk update.³

On May 12, 2021, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity* to improve the government's efforts to identify, deter, protect against, detect, and respond to cyber threats.⁴ The issuance of the order was prompted, in part, by malicious cyber campaigns threatening the public and private sectors, including an individual incident that targeted the federal government in December 2020.⁵

The Federal Information Security Modernization Act of 2014 (FISMA) includes a provision for us to periodically report to Congress on federal agencies' progress in implementing information security practices that strengthen their cybersecurity. Our specific objectives for this report were to determine to what extent (1) agencies have implemented the leadership and oversight-related requirements in the order, and (2) the order has addressed federal cybersecurity challenges.

For our first objective, we identified 115 provisions in the order. We then removed a subset of provisions from scope that did not require an action with government-wide leadership or oversight focus. Also, if the actions taken in two provisions were dependent on each other, we considered them as one combined requirement. As a result of these steps, we narrowed the focus of our review to 55 leadership and oversight requirements.

We then identified three key agencies that were assigned to perform the leadership and oversight requirements: the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB). In addition to these three,

³GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023).

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

⁵This incident, known as the SolarWinds incident, is considered one of the most significant cyber campaigns ever conducted against federal government systems. For more details, see GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, [GAO-22-104746](#) (Washington, D.C.: Jan. 13, 2022).

a fourth agency, the Office of the National Cyber Director (ONCD) is responsible for overall implementation of the order and its requirements.

We then analyzed the extent to which each of these 55 requirements were completed. Fully completed requirements were those where the actions required were deemed complete. Partially completed requirements were those where we assessed significant progress to be made in completing a requirement. Requirements considered to be not complete were those where the progress made toward completion was minimal and not significant. We conducted this review by analyzing guidance, memoranda, interviews, reports, and contract language.

For our second objective, we used the GAO High-Risk Series reports to identify a list of 10 federal cybersecurity critical actions that agencies need to take to address the four major cybersecurity challenges that the federal government faces.⁶ We then conducted a small group session with six federal chief information security officers (CISO) to get their perspectives on the 10 critical actions, and the extent to which CISOs found taking these actions to be challenging in their day-to-day operations.⁷ We also asked them to identify cyber-related areas, if any, that they consider to be challenges to their agencies' cyber operations.

We then analyzed which of the identified actions or areas were addressed by the order. Specifically, we compared the 10 cyber critical action areas listed in GAO's High-Risk Series report, as well as the additional cyber-related areas mentioned by CISOs, against the text of the order's requirements. For any areas not addressed by the order, we considered whether other recently issued government frameworks, strategies, or guidance was likely to address them. See appendix I for further information on our objectives, scope, and methodology.

We conducted this performance audit from October 2022 to April 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

⁶GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021) and [GAO-18-622](#).

⁷Specifically, the CISOs we spoke with were from the Departments of Commerce, Education, and Homeland Security and at the General Services Administration, National Aeronautics and Space Administration, and Office of Personnel Management. These CISOs were identified by the federal CISO Council as having relevant experience regarding the executive order and were able to participate in the discussion.

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.

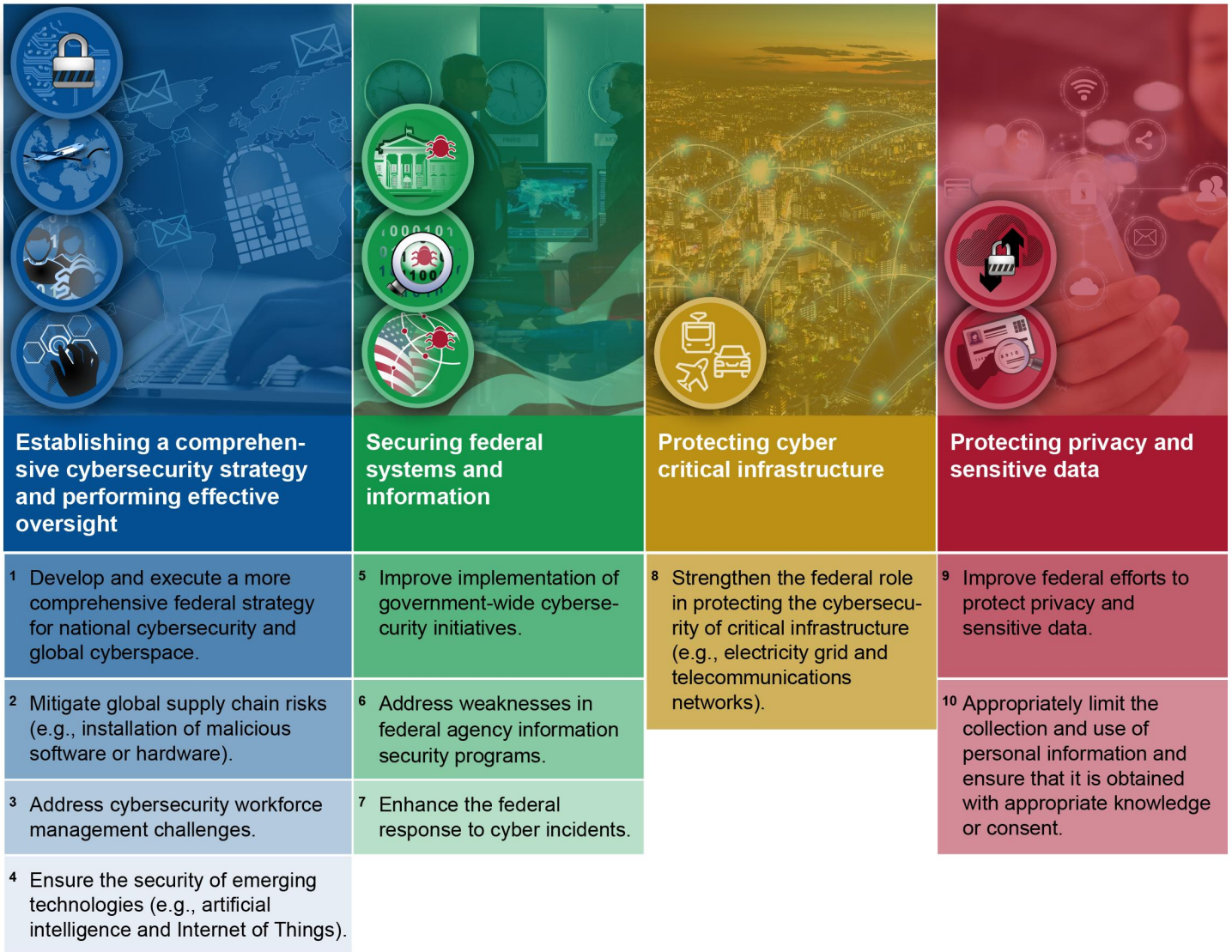
Background

Federal agencies are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Therefore, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to, among other things, obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

In September 2018, as part of its High-Risk Series, GAO identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them.⁸ The major challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Figure 1 provides an overview of the major challenges and the critical actions needed to address them.

⁸[GAO-18-622](#).

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions



Sources: GAO (analysis and icons), Who is Danny (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

Accessible Data Table for Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions

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.

Establishing a comprehensive cybersecurity strategy and performing effective oversight

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.

Sources: GAO (analysis and icons), Who is Danny (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

Past Cyber Incidents Have Been Numerous

As stated previously, the order was issued, in part, to require federal agencies to take action to address cyber incidents targeting the federal government. CISA and OMB incident report data show that agencies reported an average of approximately 31,492 incidents per year for fiscal years 2017 through 2022. In fiscal year 2022, agencies reported experiencing 30,659 incidents.⁹

According to United States Computer Emergency Readiness Team incident report data, the incidents reported in fiscal year 2022 involved several threat vectors.¹⁰ These included improper usage by an authorized user, e-mail/phishing attacks, attacks executed from a website or web-based application, and loss or theft of a computing device or media. Recent major cyber incidents include the following:

- In December 2021, a vulnerability was discovered in the Apache Log4j framework.¹¹ Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information.¹² Thus, this vulnerability could have potentially affected every organization with a networked component. As of July 2022, no significant attacks on federal critical infrastructure using the Log4j vulnerability have been reported. However, instances of the vulnerable software are likely to remain for years.

⁹Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report*, Fiscal Year 2022 (Washington, D.C.: May 1, 2023); *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2020 (Washington, D.C.: May 21, 2021); *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2018 (Washington, D.C.: August 2019).

¹⁰A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack.

¹¹In December 2021, a vulnerability was discovered in the Apache Log4j framework, which is a type of cyber security logging software used in websites and web applications across the world. The vulnerability, if left unmitigated, could allow malicious individuals to break into online-based systems, including cloud services and applications, to compromise data.

¹²The National Institute of Standards and Technology defines operational technology as programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment.

-
- In December 2020, OMB reported a breach of SolarWinds' (a network management software company) Orion software.¹³ In February 2020, a threat actor began injecting hidden code into a file that was later included in SolarWinds Orion software updates. Since the software was widely used in the federal government to monitor network activity on federal systems, this incident allowed the threat actor to breach infected agency information systems. SolarWinds estimated that nearly 18,000 of its customers received a compromised software update. This breach was considered one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector.

Order Issued in Response to Persistent Cyber Incidents

On May 12, 2021, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity*, to improve the federal government's response to cybersecurity threats, especially those caused by sophisticated malicious cyber campaigns. It called for a partnership with the private sector to secure IT systems and systems that run machinery that is used to ensure public safety—operational technology—through implementation of a series of standards and requirements.

According to staff at CISA, OMB and ONCD, the President issued the order to modernize and evolve security practices, such as those in FISMA, to better protect against current threats.¹⁴ Among other things, these threats were evidenced by recent high-profile breaches, and included increased persistent threats by sophisticated state actors, and issues in sufficiently authorizing new uses of cloud services across federal government cyber networks. An ONCD staff member also stated that the intent of the order is to aggressively change the federal government's cybersecurity culture to center around leading practices in

¹³See [GAO-22-104746](#).

¹⁴The *Federal Information Security Modernization Act of 2014* (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as *Title III, E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

cybersecurity, especially in avoiding traditional perimeter-based defenses and incorporating security by design.¹⁵

The order is split into 11 sections. Eight of the 11 sections contain required actions for federal agencies to perform toward achieving a specific cybersecurity goal, while the other three sections supply context and supporting information.¹⁶ All actions with a specified completion date were required to be completed by May 2022. Figure 2 gives an overview of the 11 sections. Each of the order's sections are also listed in their entirety in appendix II.

¹⁵According to CISA, security by design products are those products where security elements are built in during a product's design phase, rather than added after a product is fully developed. The purpose of using secure by design principles is to reduce the number of exploitable flaws before products are introduced to the market for broad use or consumption.

¹⁶The three sections of the order containing context and supporting information include: section one (introduces the executive order's purpose), section 10 (defines key terms), and section 11 (provides context for other relevant laws related to the order).

Figure 2: Overview of Executive Order 14028 Sections

- 

1 Policy. An introductory section that does not contain any requirements for agencies. It states that all federal systems should meet or exceed the standards set forth in the order.
- 

2 Removing barriers to sharing threat information. Focuses on removing contractual barriers to increase the sharing of information on cyber threats, incidents, and risks.
- 

3 Modernizing federal government cybersecurity. Focuses on modernizing the federal government's approach to cybersecurity, and increasing its visibility into cyber threats.
- 

4 Enhancing software supply chain security. Focuses on actions the federal government must take to rapidly improve the security and integrity of the software supply chain.
- 

5 Establishing a cyber safety review board. Focuses on a public-private board to review significant cyber incidents.
- 

6 Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents. Focuses on standardized response processes for identifying, remediating, and recovering from vulnerabilities and incidents affecting federal systems.
- 

7 Improving detection of cybersecurity vulnerabilities and incidents on federal government networks. Focuses on employing resources and authorities to maximize the early detection of cyber vulnerabilities and incidents on federal government networks.
- 

8 Improving the federal government's investigative and remediation capabilities. Focuses on increasing agencies' ability to collect and maintain information from network and system logs on federal information systems.
- 

9 National security systems. Focuses on the application of requirements in the order to national security systems.
- 

10 Definitions. Focuses on defining key terms, concepts, and entities used within the order.
- 

11 General Provisions. Clarifies the order's effect on previously established laws and procedures. It also states that the order might be modified later to accommodate a role for the Office of the National Cyber Director (ONCD) in executing the order. ONCD was not yet fully established at the time the order was issued.

Sources: GAO analysis of Executive Order 14028, *Improving the Nation's Cybersecurity*; marinashevchenko/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

Executive Order	Section
1	Policy. An introductory section that does not contain any requirements for agencies. It states that all federal systems should meet or exceed the standards set forth in the order.

Letter

Executive Order	Section
2	Removing barriers to sharing threat information. Focuses on removing contractual barriers to increase the sharing of information on cyber threats, incidents, and risks.
3	Modernizing federal government cybersecurity. Focuses on modernizing the federal government's approach to cybersecurity and increasing its visibility into cyber threats.
4	Enhancing software supply chain security. Focuses on actions the federal government must take to rapidly improve the security and integrity of the software supply chain.
5	Establishing a cyber safety review board. Focuses on a public-private board to review significant cyber incidents.
6	Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents. Focuses on standardized response processes for identifying, remediating, and recovering from vulnerabilities and incidents affecting federal systems.
7	Improving detection of cybersecurity vulnerabilities and incidents on federal government networks. Focuses on employing resources and authorities to maximize the early detection of cyber vulnerabilities and incidents on federal government networks.
8	Improving the federal government's investigative and remediation capabilities. Focuses on increasing agencies' ability to collect and maintain information from network and system logs on federal information systems.
9	National security systems. Focuses on the application of requirements in the order to national security systems
10	Definitions. Focuses on defining key terms, concepts, and entities used within the order.
11	General Provisions. Clarifies the order's effect on previously established laws and procedures. It also states that the order might be modified later to accommodate a role for the Office of the National Cyber Director (ONCD) in executing the order. ONCD was not yet fully established at the time the order was issued.

Sources: GAO analysis of Executive Order 14028, Improving the Nation's Cybersecurity; [marinashevchenko/stock.adobe.com](https://www.whitehouse.gov) (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

The order contains a total of 115 identified provisions spread across the eight sections of the order containing required cybersecurity actions for federal agencies. The order assigns a lead agency for each required action. Table 1 shows the number and types of responsibilities that were assigned to a lead agency or entity.

Table 1: Number and Types of Responsibilities Assigned for Actions in Executive Order 14028

Lead Agency or Entity	Number of lead responsibilities assigned	Examples of assigned responsibilities
Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA)	30	Set requirements and develop frameworks and procedures for agencies to follow and use; evaluate criticality of software used by federal agencies; provide recommendations to agencies on how to initiate cyber actions, and to others on contract language and incident management; establish cyber board
Federal agencies ^a	13	Update agency-specific cyber contractual requirements for cyber incident reporting; adopt and comply with requirements for endpoint detection and response (EDR), zero trust architecture (ZTA), event logging and National Institute of Standards and Technology (NIST) guidance regarding software supply chain
Department of Commerce/NIST	13	Publish guidance that identifies best practices and enhances the security of the software supply chain and critical software; conduct pilot programs and identify criteria for software labeling programs and Internet of Things cybersecurity
Office of Management and Budget/Administrator for Office of E-Government	12	Recommend contract language and requirements with service providers to the Federal Acquisition Regulatory Council, and incorporate into annual budget a cost analysis; require agencies to comply with NIST guidance of software supply chain and critical software; provide resources for agencies to comply with requirements of EDR, ZTA, and event logging
Department of Defense/National Security Agency	7	Develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies; recommend appropriate actions for improving detection of cyber incidents affecting national security systems; establish procedures with DHS to immediately share orders or directives applying to their respective information networks, and evaluate whether to adopt guidance contained in an order or directive
Federal Acquisition Regulatory Council	4	Amend recommendations of contract language requiring suppliers to share cyber threat and incident information, report information that will facilitate incident response and remediation, standardize agency-specific contract language, and enhance the security of software supply chain
Cyber Safety Review Board	3	Review, assess and provide recommendations for improving cybersecurity and incident response affecting federal and non-federal systems
Information and communication technology service providers	2	Report to federal agencies and CISA cyber incidents that involve a software product or a support system provided to such agencies
Office of the Director for National Intelligence	2	Develop procedures and recommend actions improving cyber incident reports affecting national security systems

Lead Agency or Entity	Number of lead responsibilities assigned	Examples of assigned responsibilities
General Services Administration Federal Risk and Authorization Management Program (FedRAMP)	1	Modernize FedRAMP, including establishing agency training programs on its use, in addition to streamlining documentation and the use of frameworks
Department of Justice	1	Develop procedures and recommend actions to improve cyber incident reports affecting national security systems
Committee on National Security Systems	1	Review recommendations and establish procedures for improving detection of cyber incidents affecting national security systems

Source: GAO analysis of information in Executive Order 14028. | GAO-24-106343

Note: Within the order, responsibility for implementing a required action can be allocated to more than one entity. Thus, the total number of responsibilities in this table is higher than the total number of provisions.

^aThis category includes responsibilities assigned to federal civilian executive branch agencies. According to Executive Order 14028, the term “federal civilian executive branch agencies” includes all agencies except for the Department of Defense and agencies in the Intelligence Community.

Four Agencies Perform Executive Order Leadership and Oversight Activities

Among its 115 provisions, the order contains 55 leadership and oversight requirements (actions to assist or direct the federal agencies in implementing the order).¹⁷ The full text of all responsibilities in the order can be found in appendix II.

Seven of the order’s sections contain leadership and oversight requirements, with DHS’s CISA, NIST, and OMB having responsibility for these requirements.¹⁸ The responsibilities assigned to these agencies are reflective of their individual missions. For example:

¹⁷In some instances, multiple Executive Order provisions have output dependent on each other to constitute one leadership/oversight requirement.

¹⁸As stated previously, eight sections of the order contain required cybersecurity actions for federal agencies. The order’s leadership and oversight requirements are contained within seven of these sections, which are sections 2 through 8.

These requirements reflect similar responsibilities given to DHS and OMB in overseeing agencies’ cyber risk management efforts, and to CISA in working with agencies on incident management capabilities. See GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, [GAO-21-236](#) (Washington, D.C.: Mar. 10, 2021) and *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, [GAO-19-384](#) (Washington, D.C.: Jul. 25, 2019).

- CISA’s mission is to lead efforts to understand, manage, and reduce risk to the nation’s cyber and physical infrastructure. CISA officials stated that the agency’s leadership and oversight responsibilities in the order include reviewing existing policies and recommending changes that align with the order’s requirements, creating reference documents, and providing implementation guidance to agencies.
- NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST officials stated that its leadership role in implementing the order is consistent with its longstanding role to develop and publish cybersecurity standards and guidelines for government and industry.
- OMB’s mission is to assist the President in meeting policy, budget, management, and regulatory objectives and to fulfill its own statutory responsibilities. OMB staff stated that its leadership and oversight role in implementing the order is related to its government-wide role in overseeing agency compliance with FISMA and coordinating the efforts of federal agencies with those of its other partners.

In addition to the three agencies identified in the executive order with leadership responsibilities, in March 2022, ONCD assumed overall responsibility over tracking the order’s requirements to completion.¹⁹ These responsibilities include assessing agency implementation of national cyber priorities, reviewing agency responses to these priorities, and identifying potential solutions to any gaps in agency responses. They also include providing feedback to agencies on whether their priorities are consistent with overall federal cybersecurity strategy.

Agencies Implemented Most of the Order’s Leadership and Oversight Requirements

CISA, NIST, and OMB have made significant progress in implementing Executive Order 14028’s leadership and oversight requirements. Together, these agencies have fully implemented 49 of the 55 leadership and oversight requirements, partially completed five, and one was not

¹⁹When the order was developed in May 2021, it included a provision to allow some of the responsibilities to be transferred to ONCD. Subsequently, in early 2022, ONCD took on its current oversight responsibility over the order’s implementation. According to ONCD staff, the office did not participate in the development of the order.

applicable. For example, they have developed procedures for improving the sharing of cyber threat information, guidance on security measures for critical software, and a playbook for conducting incident response. Moreover, ONCD, in its role as overall coordinator of the order, collaborated with agencies regarding specific implementations and tracked implementation of the order. However, a handful of requirements remain incomplete, including defining a list of critical software products, and documenting assistance to agencies in adequately resourcing the order. Table 2 shows the extent to which CISA, NIST, and OMB have implemented the leadership and oversight requirements in each section of the order.

Table 2: Progress in Implementing Executive Order 14028 Leadership and Oversight Requirements, as of March 2024

Executive Order Section	Fully Completed	Partially Completed	Not Completed	Not Applicable
Removing Barriers to Sharing Threat Information	6	1	no requirements received this score	no requirements received this score
Modernizing Federal Government Cybersecurity	8	no requirements received this score	no requirements received this score	no requirements received this score
Enhancing Software Supply Chain Security	16	1	no requirements received this score	no requirements received this score
Establishing a Cyber Safety Review Board	6	1	no requirements received this score	no requirements received this score
Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	4	no requirements received this score	no requirements received this score	1
Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks	7	1	no requirements received this score	no requirements received this score
Improving the Federal Government’s Investigative and Remediation Capabilities	2	1	no requirements received this score	no requirements received this score
Total	49	5	no requirements received this score	1

Legend:

Fully completed: Those where the actions required are complete

Partially completed: Those where significant, but not complete, progress was made in completing a requirement

Not completed: Those where the progress made toward completion was minimal and not significant

Not applicable: Agency progress is not applicable for this requirement due to its timing with respect to other requirements

The symbol “—” indicates that no requirements received this score.

Source: GAO analysis of documentation from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency; the National Institute of Standards and Technology; and the Office of Management and Budget. | GAO-24-106343

Note: Sections two through eight of the order contain leadership and oversight requirements, while the others include contextual information.

The following sections further detail agency progress in implementing requirements in each of the seven sections of the order containing leadership and oversight responsibilities.

Removing Barriers to Sharing Threat Information

Section 2 of the order addressed removing contractual restrictions that may limit the sharing of threat information and response efforts with appropriate executive departments and agencies. Among other things, it includes recommending updates to contract language to the Federal Acquisition Regulatory Council. These recommended updates are related to the monitoring of agency networks for threats and sharing reports of cyber incidents with service providers and agencies. Both OMB and CISA are responsible for creating a portion of the new contract language; subsequently, CISA is required to work with each agency to develop agency-specific cyber requirements.

Of the seven requirements in this section, the agencies fully implemented six and partially implemented one. Table 3 illustrates the status of each of the requirements in section 2.

Table 3: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Removing Barriers to Threat Information, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Review contract requirements for service providers and recommend updates to requirements and language in the contracts	CISA	Fully implemented
Ensure that service providers share data on cyber threats, incidents, and risks, to the greatest extent possible	CISA/OMB	Fully implemented
Manage information reported by agency-contracted service providers when they discover a cyber incident involving a product or service provided to an agency	CISA	Fully implemented
Recommend contract language on the nature of cyber incidents requiring reporting	CISA	Fully implemented
Develop, with input from other agencies, procedures for ensuring that cyber incident reports are shared among agencies	CISA	Fully implemented
Review agency-specific cyber requirements that exist and recommend standardized contract language	CISA	Fully implemented
Incorporate into annual budget process a cost analysis of the steps to be taken in this section	OMB	Partially implemented

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA) and Office of Management and Budget (OMB). | GAO-24-106343

CISA and OMB fully implemented all but one of the order's requirements in this section.²⁰ Among other things:

- CISA submitted contract clauses and recommendations that emphasized a government-wide approach to sharing cyber incident information to the Federal Acquisition Regulatory Council for review. In October 2023, the council published a proposed rule based on the information in these contract clauses.²¹
- CISA and OMB have taken steps to ensure that service providers share needed data on cyber threats, incidents, and risks. For example, in September 2021, CISA and OMB issued a joint statement that a major service provider would share its information on cyber incidents and threat actors with federal agencies.
- CISA developed procedures to help ensure cyber incident reports are shared among agencies. For example, CISA jointly developed procedures with the Department of Justice, the Office of the Director of National Intelligence, and the National Security Agency to enhance the sharing of incident reports developed by service providers. Among other things, these procedures identified information that CISA must receive from service providers and share with its federal partners, and the timeframes in which CISA should share this information.

However, OMB partially implemented a requirement to incorporate a cost analysis of these steps into its annual budget process. Specifically, OMB issued a memorandum in July 2022 which outlined the Administration's cybersecurity priorities for the fiscal year 2024 budget.²² Staff stated that they guided agencies in creating accurate budget estimates for implementing the order, and that these funding priorities supported the order's emphasis on improving information sharing between the federal government and private sector. However, OMB did not provide evidence

²⁰For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

²¹88 Fed. Reg. 68055-68067 (Oct. 3, 2023). The proposed rule requests that comments be provided by December 2023 for consideration in the final rule.

²²See Office of Management and Budget, Office of the National Cyber Director, *Administration Cybersecurity Priorities for the FY 2024 Budget*, M-22-16 (Washington, D.C.: July 22, 2022). OMB prepares a proposed budget on behalf of the President containing the budget message from the President to the Congress, information on the President's priorities, and summary tables. The budget must include detailed information and analysis specifically pertaining to cybersecurity initiatives, including the most recent risk assessment and summary of cybersecurity needs in each initiative area. See 31 U.S.C. 1105(a)(35).

that it had incorporated an analysis of specific costs agencies would incur in implementing recommendations made by CISA related to the sharing of cyber threat information into the government's annual budget process.

An OMB staff member stated that the requirement to incorporate this cost analysis was met through communication with agencies on cybersecurity funding priorities in each fiscal year. Additionally, they stated that OMB works with agency resource management offices to manage each agency's cost analysis information. Furthermore, the staff member stated that OMB held regular one-on-one follow-up communications to discuss specific implementation costs on an agency-by-agency basis.

Nonetheless, OMB could not demonstrate that its communications with pertinent federal agencies included a cost analysis for implementation of recommendations made by CISA related to the sharing of cyber threat information. Documenting the results of communications between federal agencies and OMB would increase the likelihood that agency budgets are sufficient to implement these recommendations. For example, OMB could consider including the results in its proposed budget on behalf of the President, which contains, among other items, analytical perspectives designed to highlight specified subject areas or provide other significant presentations of budget data that place the budget in perspective. Without documenting these results, OMB may not be able to ensure that each agency's needs are effectively represented in their annual budget requests.

Modernizing Federal Government Cybersecurity

Section 3 of the order addressed modernizing the federal government's approach to cybersecurity and increasing its visibility into threats while protecting privacy and civil liberties. Among other things, it includes taking steps towards implementation of zero trust architecture, securing cloud services and centralizing access to cybersecurity data.

As seen in Table 4, CISA and OMB fully implemented all eight leadership and oversight requirements in this section.

Table 4: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Modernizing Federal Government Cybersecurity, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Receive information from agencies regarding their plans to implement zero trust architecture	OMB	Fully implemented
Provide guidance to agencies that move closer to implementing zero trust architecture and ensure that the risk from using cloud-based services is addressed	OMB	Fully implemented
Develop and issue for agencies a cloud security technical reference architecture documentation	CISA	Fully implemented
Develop a cloud-service governance framework that identifies a range of services and protections available to agencies based on incident severity, as well as data and processing activities	CISA	Fully implemented
Receive evaluation reports from agencies on the types and sensitivity of their respective unclassified data	CISA	Fully implemented
Receive reports from agencies on progress in adopting multifactor authentication and encryption of data at rest and in-transit, and take all appropriate steps to maximize adoption by agencies	CISA	Fully implemented
Receive a written rationale from all agencies that are unable to fully adopt multifactor authentication and data encryption within the prescribed date	CISA	Fully implemented
Establish a framework to collaborate on cybersecurity and incident response activities related to cloud technology	CISA	Fully implemented

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA) and Office of Management and Budget (OMB). | GAO-24-106343

CISA and OMB fully implemented the order’s requirements related to modernizing federal government cybersecurity.²³ Among other things:

- In fiscal year 2022, OMB and CISA confirmed that they received and subsequently reviewed zero trust architecture implementation plans from 70 agencies. OMB and CISA also held guidance sessions to ensure that agencies took steps toward implementing their plans, including assessing their cyber environments in preparation for the implementation, and ensuring they understood the resources needed.
- In January 2022, OMB issued a memorandum which set up specific cybersecurity standards for implementing zero trust architecture.²⁴ For example, the memorandum required agencies to employ centralized identity management systems for users, integrate and enforce multifactor authentication across applications, and maintain a

²³For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

²⁴Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

complete inventory of every device authorized and operated for official business.²⁵

Enhancing Software Supply Chain Security

Section 4 of the order addressed enhancing mechanisms to ensure that software used by federal supply chain partners, especially those performing critical functions, has sufficient security and integrity. This includes issuing standards and procedures that enhance the security of the software supply chain, as well as implementation of these measures for legacy systems. The requirements also include producing recommendations for minimum standards for vendor testing of software source code.

Of the 17 requirements in this section, agencies fully implemented 16 and partially implemented one. Table 5 illustrates the status of each of the leadership and oversight requirements in section 4.

Table 5: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Enhancing Software Supply Chain Security, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Solicit input and publish preliminary guidelines to enhance the security of the software supply chain	NIST	Fully implemented
Update guidelines and publish additional procedures for periodic review to enhance software supply chain security	NIST	Fully implemented
Issue guidance identifying practices that enhance the security of the software supply chain. Guidance shall identify standards, procedures, and criteria such as establishing multifactor, risk-based authentication	NIST	Fully implemented
Publish the definition of the term “critical software”	NIST	Fully implemented
Identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of “critical software”	CISA	Partially implemented
Publish guidance outlining security measures for “critical software”	NIST	Fully implemented
Require agencies to comply with guidance outlining security measures for “critical software”	OMB	Fully implemented
Require agencies to comply with guidelines for enhancing the security of the software supply chain for software procured after the date of Executive Order 14028	OMB	Fully implemented
Identify and explain all extensions or waivers granted to agencies for not complying with requirements to enhance software supply chain security for all software procured after the date of the order and report these on a quarterly basis	OMB	Fully implemented

²⁵Identity management involves authenticating subjects, such as persons or devices, that use federal resources. See Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, M-19-17 (Washington, D.C.: May 21, 2019).

Requirement in Executive Order 14028	Agency	Implementation Status
Recommend to the Federal Acquisition Regulatory Council contract language requiring suppliers of software available for purchase by agencies to comply with guidance that enhances the security of the software supply chain	CISA	Fully implemented
Require agencies employing software developed and procured prior to Executive Order 14028, including legacy software, to provide a plan outlining action to remediate or meet those requirements issued in this section	OMB	Fully implemented
Publish guidelines recommending minimum standards for vendor testing of software source code	NIST	Fully implemented
Initiate pilot programs, consistent with existing guidance and informed by existing consumer product labeling programs, to educate the public on the security capabilities of Internet of Things devices and software development practices	NIST	Fully implemented
Identify Internet of Things cybersecurity criteria for a consumer labeling program, and consider whether a consumer labeling program may be operated in conjunction with or modeled after any similar government programs	NIST	Fully implemented
Identify secure software development practices or criteria for a consumer software labeling programs and consider whether a consumer software labeling program may be operated in conjunction with or modeled after any similar government programs	NIST	Fully implemented
Conduct a review of the pilot programs and submit a summary report to the Assistant to the President for National Security Affairs	NIST	Fully implemented
Provide the President, through the Assistant to the President for National Security Affairs, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain	NIST	Fully implemented

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB). | GAO-24-106343

NIST and OMB fully implemented all of the leadership and oversight requirements related to enhancing software supply chain security. CISA fully implemented all but one of these requirements.²⁶ Among other things:

- In July 2021, NIST published guidelines for identifying practices that enhance the security of the software supply chain and for evaluating the security practices of developers and suppliers of critical software.²⁷ For example, the guidelines included guidance to organizations for identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels within their organization.

²⁶For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

²⁷National Institute of Standards and Technology, *Special Publication SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (Gaithersburg, Md.: May 2022); *Security Measures for “EO-Critical Software” Use* (Gaithersburg, Md.: Jul. 8, 2021). The order defines critical software as software that performs functions critical to trust. This could include software that allows or requires elevated system privileges or direct access to networking and computing resources.

- In February 2022, NIST published guidance outlining security measures for critical software. Among other things, NIST identified key practices such as defining key performance indicators and other criteria for determining software security; segregating software development environments; and making integrity verification information available to those responsible for software acquisition.
- In September 2022, OMB issued a memorandum instructing agencies on the use of secure software development practices to secure their supply chains.²⁸ This memorandum instructed agencies on actions and timelines for steps to secure their supply chain according to the NIST guidelines, including for legacy software. In March 2024, CISA and OMB issued a software development attestation form to further guide agencies on required actions in this area.

However, CISA partially implemented the remaining requirement related to supply chain security. Specifically, CISA and OMB assisted NIST in developing the criteria and guidelines for required federal government software security measures. Additionally, CISA, OMB, and NIST developed a definition of critical software and a preliminary list of common categories of software that are consistent with that definition.

Nevertheless, CISA has not issued the list. An official stated that the agency had extensive concerns about the completeness and quality of the data available to develop the list of software categories. The official also stated that CISA was concerned about how agencies and private industry would interpret the list and planned to review existing criteria needed to validate categories of software.

A CISA official stated they planned to publicly issue a new version of the category list and a companion document that better explains its content. However, CISA did not meet its planned timeline of September 2023 for issuing this list and has not defined a new timeline. Without publishing and making available an authoritative list in a timely manner, agencies cannot be assured that software vendors are following required criteria and guidelines to enhance the security of the software supply chain.

²⁸Office of Management and Budget, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, M-22-18 (Washington, D.C: Sept. 14, 2022).

Establishing a Cyber Safety Review Board

Section 5 of the order establishes the Cyber Safety Review Board, a multi-agency board with representation from the public and private sectors. The board is required to review threat activity, vulnerabilities, mitigation activities, and agency responses for recent significant cyber incidents. The board's requirements also include reviews of the government response to a specific cyber breach, and of the board's own operations to improve its efficiency.

Of the seven requirements in this section, CISA or the board fully implemented six and partially implemented one. Table 6 illustrates the status of each of the leadership and oversight requirements related to the board's operations.

Table 6: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Establishing a Cyber Safety Review Board, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Establish a Cyber Safety Review Board (board) comprised of representatives from the federal government and private-sector cybersecurity or software suppliers. Biennially extend the life of the board and designate a Chair and Deputy Chair unless otherwise directed by the President	CISA	Fully implemented
Convene the board to review and assess significant cyber incidents affecting federal civilian executive branch information systems or non-federal systems	CISA	Fully implemented
Convene the board to perform an initial review that shall relate to the cyber activities that prompted the establishment of a Cyber Unified Coordination Group in December 2020. ^a The board shall provide recommendations to the Department of Homeland Security for improving cybersecurity and incident response practices based on this review.	CISA	Fully implemented
Confirm that the board protects sensitive law enforcement, operational, business, and other confidential information that has been shared with it	CISA	Fully implemented
Provide the President with any advice, information, or recommendations of the board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident	CISA	Fully implemented
Provide the President with recommendations for improving the board's operations	CISA	Fully implemented
Review the recommendations provided to the President for improving the board's operations and take steps to implement them as appropriate	CISA	Partially implemented

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA). | GAO-24-106343

^aThis Unified Coordination Group was created to coordinate the federal government's response to the SolarWinds incident on December 16, 2020.

CISA implemented several of the requirements in this section.²⁹ Among other things:

- In February 2022, DHS, through CISA, established the Cyber Safety Review Board. The board is comprised of representatives from the private sector and federal government. After reviewing each incident, the chair of the board is required to deliver a report with finding(s) and recommendation(s) to the Director of CISA and Secretary of DHS.
- In July 2022, the board completed an incident review of the Log4j event that occurred in December 2021.³⁰ According to CISA

²⁹For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

³⁰In December 2021, a vulnerability was discovered in the Apache Log4j framework, which is a type of cyber security logging software used in web applications across the world. The vulnerability, if left unmitigated, could allow malicious individuals to attack and exploit IT systems, including cloud services and applications.

For more details on this review, see Cyber Safety Review Board, *Review of the December 2021 Log4j Event* (Jul. 11, 2022).

documentation, the board made 19 recommendations related to this review. Common themes of the board's recommendations include developing capabilities to report continued observation of exploitation of the Log4j vulnerability; adopting industry-accepted practices for security hygiene; and researching cultural and technology shifts necessary to improve the nation's digital security.

- The federal government performed a review of the cyber activities that prompted the establishment of a Cyber Unified Coordination Group in December 2020—the SolarWinds incident. This review included a timeline of events, details on the vulnerability that was exploited, agency responses, and mitigation activities.³¹ In addition, the board provided a report to the Department of Homeland Security for improving cybersecurity and incident response practices based on the Log4j review, which included information on the SolarWinds review.
- In October 2022, the board provided operational recommendations to the President to consider adjustments to the board's composition and operations, based on lessons learned from its first incident review. Among other things, the board recommended that legislation be enacted to codify the board and its authority; that the board establish additional formal protocols and procedures to guide the management of an incident review; and that the board establish methods for the collection of information through public data calls.
- In August 2023, the board issued another report based on its review of the activities of a global extortion-focused threat actor group known as Lapsus\$.³² Common themes for the board's recommendations in response to this incident include strengthening practices for identity and access management; mitigating vulnerabilities at telecommunications providers and resellers; and building cyber resiliency by investing in prevention, response, and recovery capabilities.

However, CISA partially implemented one requirement related to the board's operations and output. Specifically, while CISA officials stated the agency has taken steps to improve the board's operations, CISA has not yet demonstrated that it has done so. According to the order, after the

³¹GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, [GAO-22-104746](#) (Washington, D.C.: Jan. 13, 2022).

³²According to the board, this group, known as Lapsus\$, exploited systemic ecosystem weaknesses to infiltrate and extort organizations for attention and public notoriety.

For more details on this review, see Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus\$ and Related Threat Groups* (Jul. 24, 2023).

board's initial cyber incident review regarding the Log4j incident was completed, the board was required to make recommendations for improving its future operations. This included areas such as membership, data access, practices for protecting information provided, and thresholds for triggering subsequent reviews. The order then required CISA to review these recommendations and take steps to implement them as appropriate.

After the board's review of the Log4j incident, the board identified operational challenges and made recommendations to mitigate them. For example, the board recommended establishing additional protocols and procedures to manage requests for information and reviews of classified material, and to interview candidates for board membership.

CISA officials stated that it has made progress in implementing the board's recommendations and is planning further steps to improve the board's operational policies and procedures. However, CISA has not provided evidence that it is implementing these recommendations. Without CISA's implementation of the board's recommendations, the board may be at risk of not effectively conducting its future incident reviews.

Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

Section 6 of the order focuses on the creation of a standard set of operational procedures, known as a playbook, for conducting cybersecurity vulnerability and incident response activities for agency information systems. The requirements include annual updates to the playbook; the creation of guidance for its use; and a review of agencies' incident response and remediation readiness upon implementation of the playbook.

Of the five requirements in this section, CISA and OMB have fully implemented four, and one was determined to be not applicable.³³ Table 7 illustrates the status of each of the leadership and oversight requirements in section 6.

³³We determined one recommendation to be not applicable because no actions are currently required on the part of the agency responsible for it.

Table 7: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Standardizing the Federal Government’s Playbook, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Develop a standard set of operational procedures, or playbook, to be used in planning and conducting a cybersecurity vulnerability and incident response activity to be used by agencies. To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms	CISA	Fully implemented
Issue guidance to agencies on use of the playbook	OMB	Fully implemented
Consult with agencies on any deviations from the playbook and require them to demonstrate that any deviations meet or exceed the standards proposed in the playbook	OMB	Not applicable
Review and update the playbook annually and provide information to OMB to incorporate in guidance updates	CISA	Fully implemented
Establish a requirement to review and validate agencies’ incident response and remediation results upon an agency’s completion of incident response activities	CISA	Fully implemented

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA), and Office of Management and Budget (OMB). | GAO-24-106343

⁹The order focuses only on what should happen if agencies request a deviation. Since no agencies have requested deviations, no actions are required on the part of OMB, and this requirement is currently not applicable.

CISA and OMB implemented all applicable requirements in this section.³⁴ Among other things:

- In November 2021, CISA published the *Cybersecurity Incident and Vulnerability Response Playbook* for agencies to use in planning and conducting cybersecurity vulnerability and incident response activities.³⁵ In the playbook, CISA developed a standard process and procedures to facilitate better coordination and effective incident response among affected organizations. The process and procedures are also intended to enable the tracking of cross-organizational actions and allow for cataloging of incidents to better manage future events.
- In December 2021, OMB issued to agencies a memorandum with required steps for implementing the playbook.³⁶ CISA also

³⁴For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

³⁵Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems* (November 2021). In this title, FCEB stands for federal civilian executive branch agencies.

³⁶Office of Management and Budget, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, M-22-05 (Washington, D.C.: Dec. 6, 2021).

implemented a review and validation process for agencies following playbook procedures on incident response and remediation. In this process, agencies can coordinate with CISA to ensure that all appropriate incident response actions have been taken. CISA will then determine whether the incident has been adequately addressed, and if it has not, make recommendations for its closure.

- The order also requires agencies to consult with OMB to ensure that the incident response standards they are using meet or exceed the standards proposed in the playbook. According to an OMB staff member, agencies have not yet requested waivers to deviate from implementing the playbook's incident response and remediation requirements.

OMB was not able implement the order's requirement to consult with agencies on any deviations from the playbook and require agencies to demonstrate that any deviations meet or exceed the standards proposed in the playbook, because no agencies have requested deviations. Since the order focuses only on what should happen if agencies request a deviation, no actions are required on the part of OMB, and this requirement is currently considered to be not applicable.

Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

Section 7 of the order focuses on enhancing federal government resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. The requirements in this section include deployment of an endpoint detection and response (EDR) initiative to support proactive detection of cybersecurity incidents within federal government infrastructure. It also includes the creation of a report describing how threat-hunting activities can be conducted on agency networks.³⁷

Of the eight related requirements, leadership and oversight agencies fully implemented seven and partially implemented one. Table 8 illustrates the status of each of the requirements in this section.

³⁷EDR combines real-time continuous monitoring and collection of endpoint data (for example, data from networked computing devices such as workstations, mobile phones, and servers) with rules-based automated response and analysis capabilities.

Table 8: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Provide recommendation to the Office of Management and Budget (OMB) on options for implementing an endpoint detection and response (EDR) initiative	CISA	Fully implemented
Issue requirements for agencies to adopt EDR approaches, including supporting a capability for Cybersecurity and Infrastructure Security Agency (CISA) to engage in cyber hunt, detection, and response activities	OMB	Fully implemented
Ensure that agencies have adequate resources to comply with the requirements for adopting EDR approaches	OMB	Partially implemented
Establish or update Memoranda of Agreement with CISA for the Continuous Diagnostics and Mitigation program to ensure that needed data are available and accessible to CISA	CISA	Fully implemented
Provide OMB and Assistant to the President for National Security Affairs a report describing how authorities to conduct threat-hunting activities on federal civilian executive branch agency networks without prior authorization from agencies are being implemented	CISA	Fully implemented
Establish procedures for the Department of Defense (DOD) and Department of Homeland Security (DHS) to immediately share DOD incident response orders or DHS emergency directives and binding operational directives	CISA	Fully implemented
Evaluate whether to adopt any guidance contained in an order or directive issued by DOD or DHS consistent with these procedures	CISA	Fully implemented
Notify the Assistant to the President for National Security Affairs and OMB of the evaluation described in this section within seven days of receiving notice of an order or directive issued consistent with the procedures in this section	CISA	Fully implemented

Source: GAO analysis of documentation from CISA and OMB. | GAO-24-106343

CISA and OMB fully implemented all but one of the order’s requirements in this section.³⁸ Among other things:

- In June 2021, CISA provided OMB with recommendations on options for implementing an EDR initiative. Among the approaches suggested by CISA were the deployment of a commercial EDR solution across all agencies, deployment of software focused on providing CISA with government-wide visibility, and more rapid attribution of root causes for incidents that are detected.
- In October 2021, OMB issued guidance for agencies to follow in implementing EDR approaches, based on options provided by CISA.³⁹ Specifically, the OMB guidance provides implementation steps for

³⁸For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

³⁹Office of Management and Budget, *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).

agencies as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the government.

- In December 2023, CISA had established memoranda of understanding with agencies to maintain access to the data needed to conduct its Continuous Diagnostics and Mitigation (CDM) program. Specifically, the memoranda identified CDM capabilities to be implemented at each agency, such as asset management, identity and access management, and network security management. It also defined the roles and responsibilities of both CISA and the agencies in implementing and operating CDM tools, sensors, and agency dashboards.

However, while CISA demonstrated it had worked with agencies to ensure they had adequate resources to implement EDR approaches, OMB could not demonstrate it had done so. Specifically, OMB staff stated that it had incorporated EDR within its guidance to agencies for budget submissions, as well as in the list of FISMA metrics in fiscal year 2023. Staff stated that, due to the nature of FISMA reporting requirements for agencies, OMB used these metrics to shape agency resource decisions. Staff members also stated that OMB had follow-up communications to discuss resource concerns on an agency-by-agency basis. However, OMB could not demonstrate that it had documented the results of these communications.

An OMB staff member stated that, due to the large number of and decentralized nature of the conversations involved, it would not have been feasible for OMB to document the results of all EDR-related communications with agencies. However, detailing how resourcing for the EDR-related initiatives was communicated provides visibility into agencies' needs, as determined by OMB. This would include whether budgets are sufficient to fully implement EDR requirements. For example, OMB could consider including these EDR resourcing estimates in its proposed budget on behalf of the President.⁴⁰ Without these details, OMB will have less certainty that each agency will receive sufficient funding for EDR initiatives to fully implement the order's requirements in this section.

⁴⁰As noted above, OMB prepares a proposed budget on behalf of the President, which contains, among other items, analytical perspectives designed to highlight specified subject areas or provide other significant presentations of budget data that place the budget in perspective.

Improving the Federal Government’s Investigative and Remediation Capabilities

Section 8 of the order focuses on agency collection of information from network and systems logs of federal information systems for the purposes of investigation and remediation. The requirements in this section include the establishment of practices for logging, including retention and management, that can support agency security operations centers. The requirements also include ensuring sufficient access to agency logs by CISA, consistent with applicable law.

Of the three relevant requirements, leadership and oversight agencies have fully completed two and partially completed one. Table 9 illustrates the status of each of the requirements in this section.

Table 9: Status of Leadership and Oversight Requirements in Executive Order 14028 Section on Improving the Federal Government’s Investigative and Remediation Capabilities, as of March 2024

Requirement in Executive Order 14028	Agency	Implementation Status
Provide the Office of Management and Budget (OMB) recommendations on requirements for logging events and retaining other relevant data within an agency’s systems and networks. These requirements should be designed to permit agencies to share log information to the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation.	CISA	Fully implemented
Formulate policies for agencies to establish requirements for logging, log retention, and log management	OMB	Fully implemented
Work with agency heads to ensure that agencies have adequate resources to comply with requirements for logging, log retention, and log management	OMB	Partially implemented

Source: GAO analysis of documentation from the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Management and Budget (OMB). | GAO-24-106343

OMB and CISA fully implemented two requirements in this section on improving the government’s investigative and remediation capabilities.⁴¹ Specifically,

- CISA provided OMB with recommendations to develop policies for logging. Among other things, CISA’s recommendations discussed required data that agencies should collect for each log event, and user behavior analytics that agencies should implement to identify potentially malicious activity.
- In August 2021, OMB issued guidance that established a maturity model to guide agency implementation requirements for event

⁴¹For details on the implementation of all leadership and oversight requirements in the order, see appendix III.

logging.⁴² The model established four tiers of maturity for event logging to help agencies understand how to achieve full compliance with logging requirements.

However, while OMB provided guidance to agencies to improve their log retention and log management practices and capabilities, OMB did not demonstrate that it had worked with agencies to ensure they had adequate resources to implement logging, log retention, or log management. An OMB staff member stated that similar to their assistance with EDR initiatives, OMB had incorporated the use of logs within the list of FISMA metrics in fiscal year 2023. Staff stated that, due to the nature of FISMA reporting requirements for agencies, OMB used these metrics to shape agency resource decisions. The staff member also stated that OMB had had interactions with agencies on an individual basis to discuss resource concerns in this area. This staff member also stated that it was not possible to track the results of these communications because of the large number of agency communications involved.

However, detailing how resourcing for logging and log management initiatives was communicated provides visibility into agencies' needs, as determined by OMB. This would include whether budgets are sufficient to fully implement the logging and log management requirements. For example, OMB could consider including these logging and log management resourcing estimates in its proposed budget on behalf of the President.⁴³ Without detailing such information, OMB will have less certainty that each agency will receive sufficient funding for logging and log management initiatives to fully implement the order's requirements in this section.

ONCD Oversaw Implementation of the Order

As previously noted, in March 2022, ONCD assumed overall responsibility over tracking the order's requirements to completion. To fulfill this role, ONCD staff stated the office has focused on collaboration and monitoring. Specifically, the Deputy National Cyber Director for

⁴²Office 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).

⁴³As noted above, OMB prepares a proposed budget on behalf of the President, which contains, among other items, analytical perspectives designed to highlight specified subject areas or provide other significant presentations of budget data that place the budget in perspective.

Federal Cybersecurity stated that ONCD collaborated with leadership and oversight agencies. For example, at a minimum, ONCD met monthly with CISA, NIST, and OMB to discuss the progress of the order's implementation. The same official stated the office also provided regular updates to the National Security Council and other relevant agencies, including as part of OMB's quarterly reports of cyber metrics under FISMA.

Further, ONCD tracked and documented progress on each of the order's requirements. Among other things, the office maintained internal documentation on each requirement that includes: (1) the lead agency responsible, (2) specific details regarding the status of agencies' work toward completion of the requirement, (3) status of deliverables required for completion, and (4) documentation of completed deliverables. ONCD also provided information on the progress against selected requirements in the order through OMB's reporting on quarterly FISMA cyber metrics.

Existing Guidance Expected to Assist Agencies in Addressing Cybersecurity Challenges

Six selected federal agency CISOs confirmed that they considered the 10 action areas identified in GAO's High-Risk Series as critical to addressing the nation's cybersecurity threats as challenges at their agencies.⁴⁴ The requirements in Executive Order 14028 address five of the 10 critical action areas, if effectively implemented. Similarly, the other five critical action areas that are unaddressed by the order may be addressed by other recently issued governmentwide strategies, guidance, and frameworks. In addition to the 10 action areas in GAO's High-Risk Series, the six CISOs also discussed additional cyber-related issues that their agencies face. The order's requirements may also address these areas, if effectively implemented.

Agency Officials Confirmed High-Risk Action Areas as Challenges; the Order Partially Addresses Them

Six federal CISOs provided insights into current major cybersecurity challenges they are experiencing at their agencies.⁴⁵ CISOs confirmed that they considered each of the 10 action areas identified in GAO's High-Risk Series report to be challenging to implement at their agencies, with some being more challenging than others. Specifically, CISOs stated that improving federal efforts to protect privacy and sensitive data and appropriately limiting the collection and use of personal information, were challenges at their agencies. However, they stated these actions could be better addressed by focusing on the implementation of other action areas identified in GAO's High-Risk report, such as improving agency information security programs.







⁴⁴[GAO-18-622](#) and [GAO-21-288](#).

⁴⁵Specifically, the CISOs we spoke with were from the Departments of Commerce, Education, and Homeland Security and at the General Services Administration, National Aeronautics and Space Administration, and Office of Personnel Management. These CISOs were identified by the CISO Council as having relevant experience regarding the order and were able to participate in the discussion.

Because the selection of the CISOs for this study was a judgmental sample, their viewpoints are not intended to represent all federal government CISOs, and the six CISOs in our small group discussion are not representative of all federal government CISOs.

The requirements in the order address five of the 10 critical action areas from GAO's High-Risk report, if effectively implemented. Figure 3 shows which of these action areas are addressed by the order's requirements.

Figure 3: GAO’s 10 High-Risk Critical Action Areas Addressed by Executive Order 14028 (EO)

Cyber Critical Action Area	Addressed by EO
 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	○
 Mitigate global supply chain risks .	✓
 Address cybersecurity workforce management challenges.	○
 Ensure the security of emerging technologies .	✓
 Improve implementation of government-wide cybersecurity initiatives .	✓
 Address weaknesses in federal agency information security programs .	✓
 Enhance the federal response to cyber incidents .	✓
 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications network).	○
 Improve federal efforts to protect privacy and sensitive data .	○
 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.	○

Sources: GAO analysis based on Executive Order 14028, *Improving the Nation’s Cybersecurity* and icons; motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

Accessible Text for Figure 3: GAO’s 10 High-Risk Critical Action Areas Addressed by Executive Order 14028 (EO)

Cyber Critical Action Area	Addressed by EO
Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	No
Mitigate global supply chain risks .	Yes
Address cybersecurity workforce management challenges.	No
Ensure the security of emerging technologies .	Yes
Improve implementation of government-wide cybersecurity initiatives .	Yes
Address weaknesses in federal agency information security programs .	Yes
Enhance the federal response to cyber incidents .	Yes
Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications network).	No
Improve federal efforts to protect privacy and sensitive data .	No
Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.	No

Sources: GAO analysis based on Executive Order 14028, Improving the Nation’s Cybersecurity and icons; motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-106343

The order addressed the following five High-Risk action areas:

- **Global supply chain risks.** The order contains specific steps to enhance security of agency supply chains. The steps include defining what should be considered “critical software”; identifying key practices that enhance the security of supply chain software; and supplying contract language to require agency supply chain partners to perform these key practices.⁴⁶ The order directs NIST to develop guidelines that contain criteria for evaluating the software security practices of developers and suppliers. It also directs NIST to require developers and suppliers to identify tools for demonstrating conformance with secure practices to agencies and others that purchase the software.
- **Security of emerging technologies.** Several of the order’s sections focus on government-wide implementation of technologies generally considered to be emerging technologies, as part of improving overall federal cyber resilience. For example, the order directs agencies to use zero trust architecture practices to facilitate more secure use of cloud technologies. The order requires implementation of pilot programs to inform the public on the security capabilities of Internet of Things devices and software development practices. It also requires

⁴⁶Critical software is defined by the order as software that performs functions critical to trust, such as affording or requiring elevated system privileges or direct access to networking and computing resources.

the adoption of endpoint detection and response approaches to detect, hunt, and respond to cyber incidents.

- **Government-wide cybersecurity initiatives.** Among other things, the order requires agencies to provide evidence of progress in implementing multifactor authentication and encryption for data at rest and in transit, and for CISA to work with agencies to ensure consistent implementation of these technologies across agencies. The order also requires the development of memoranda of agreement to ensure that CISA has access to agencies' data for vulnerability analysis and threat hunting purposes.
- **Weaknesses in federal agency information security programs.** In addition to the development of standard vulnerability and incident response procedures for agencies to use in identifying, remediating, and recovering from incidents, the order requires CISA to establish a framework to collaborate on cybersecurity and incident response activities related to cloud technology. It also requires CISA to set up a review board to analyze details of significant cyber incidents.
- **Responses to cyber incidents.** Several of the order's sections address agency responses to cyber incidents, such as the collection and dissemination of incident data. Specifically, the order required agencies to remove communication barriers between service providers by detailing when service providers must record and share information on cyber threats and incidents with agencies. The order also required agencies to develop a standard playbook to be used by agencies when planning and conducting cybersecurity vulnerability and incident response activities.

The order does not address the other five of the 10 critical action areas. However, each of the five could potentially be addressed by other recently issued government-wide strategies, frameworks, and guidance. Specifically:

- **Strategy for national cybersecurity.** In March 2023, the White House issued the *National Cybersecurity Strategy* to coordinate efforts to secure the nation against cyber risks and threats.⁴⁷ The strategy contains five cyber-related areas, known as pillars. These pillars address areas such as limiting the effect of threat actors and partnering with the private sector to improve security and cyber resilience. Prior GAO work noted shortfalls and potential challenges in

⁴⁷White House, *National Cybersecurity Strategy* (Washington, D.C.: March 2023).

the strategy's implementation.⁴⁸ If the strategy and its accompanying implementation plan are effectively implemented to account for these shortfalls and challenges, this action area may be addressed.⁴⁹

- **Cyber workforce management.** ONCD issued the *National Cyber Workforce and Education Strategy* in July 2023, which focused on developing cyber skills, and expanding and enhancing the national cyber workforce, among other things.⁵⁰ If the goals of the strategy are fully achieved, this action area could potentially be addressed.

Five CISOs reiterated that the cyber workforce action area was one of the most significant and challenging to implement overall. CISOs also spoke to the importance of offering workplace flexibility, such as remote work and competitive pay, and an inability to hire top tier talent because they could not offer such flexibilities.

- **Cybersecurity of critical infrastructure.** While this challenge is not fully addressed in the order, the *National Cybersecurity Strategy* and its associated implementation plan also address the securing of cyber critical infrastructure.⁵¹ Specifically, the implementation plan gave responsibility to agencies in areas such as harmonizing baseline cyber requirements for critical infrastructure and further designating federal agency responsibilities for coordinating the activities of critical infrastructure sectors. If effectively implemented, the strategy and implementation plan could potentially address the challenge of cybersecurity risks to critical infrastructure.

⁴⁸GAO, *Cybersecurity: Launching and Implementing the National Cybersecurity Strategy*, [GAO-23-106826](#) (Washington, D.C: June 2023).

⁴⁹White House, *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

⁵⁰White House, *National Cyber Workforce and Education Strategy* (Washington, D.C.: July 31, 2023).

⁵¹White House, *National Cybersecurity Strategy and National Cybersecurity Strategy Implementation Plan*. The first pillar of the *National Cybersecurity Strategy* is to defend critical infrastructure. This pillar includes goals such as introducing an enduring model which distributes cybersecurity risks and responsibilities, constructing regulatory frameworks that focus on achieving cybersecurity objectives, and collaborating with private sector and state, local, tribal, and territorial partners in response to cyber incidents. The strategy outlines five strategic objectives for defending critical infrastructure, and the implementation plan details 16 initiatives for meeting the five strategic objectives.

GAO has ongoing work to assess the extent to which the implementation of the *National Cybersecurity Strategy* and its corresponding implementation plan address cybersecurity risks.

- **Protection of privacy and sensitive data, and collection and use of personal information.** Recent federal frameworks and guidance have been issued to address privacy protections. For example:
 - In 2020, NIST issued its *Privacy Framework* to help entities reduce privacy risks by helping them understand the connection between their mission, organizational roles and responsibilities, and privacy protection activities.⁵²
 - In addition, in 2020, OMB issued two memoranda to guide agencies in improving their privacy practices.⁵³ Specifically, OMB provided rules regarding the access to personal information and for appropriately disclosing information on security vulnerabilities. OMB also issued an updated circular in 2023 with specific guidance to agencies on privacy practices and obligations when creating an annual budget submission.⁵⁴

The framework and guidance documents help to provide a basis for agencies to implement good privacy practices. If effectively implemented, these documents could help agencies protect privacy and sensitive data, and appropriately limit their collection and use of personal information.

Executive Order Addresses Additional Challenges Identified by CISOs

In addition to the 10 critical action areas, CISOs discussed three cyber-related issue areas they consider to be challenges at their agencies. If effectively implemented, the order will also address these additional areas. Specifically:

- **Uncertainty in cyber funding, including an inability to protect funding for multi-year initiatives.** CISOs considered this area as one of the most significant and challenging to implement overall. Two CISOs stated that securing funding for multi-year projects was

⁵²National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (Gaithersburg, Md.: Jan. 16, 2020).

⁵³Office of Management and Budget, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, M-21-04 (Washington, D.C.: Nov. 12, 2020) and *Improving Vulnerability Identification, Management, and Remediation*, M-20-32 (Washington, D.C.: Sept. 2, 2020).

⁵⁴Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (Washington, D.C.: August 2023).

especially challenging since they are unable to efficiently plan and allocate their cyber resources, including key modernization efforts. One CISO stated that budget uncertainty caused by situations such as continuing resolutions can pause cyber modernization projects.⁵⁵

The order includes several requirements related to ensuring that agencies have sufficient resources to implement specific requirement areas. Specifically, the order requires that OMB incorporate into its annual budget decisions a cost analysis of all recommendations made to agencies regarding the sharing of cyber threat information. It also requires that OMB work with agency heads to ensure adequate resourcing to implement requirements to improve incident detection and remediation.

- **Lack of a “cyber culture” where agencies prioritize cybersecurity as an essential part of agency mission and operations.** CISOs considered this area as one of the most significant and challenging to implement overall. Four CISOs voiced concerns that agencies were left alone to develop and maintain their own cyber capabilities, despite other agencies across the government sharing the same objectives. The CISOs also stated that they would like to see cyber leadership agencies, such as CISA, provide even more extensive cybersecurity services to other agencies.

The order requires leadership and oversight agencies to collaborate with agency heads to enact several of its requirements, such as the implementation of multifactor authentication and encryption, and appropriate processing and storage solutions for each agency’s sensitive data.

- **A focus on cyber compliance in lieu of cyber resilience or operational security.** For example, one CISO discussed how, despite many layers of compliance practices they are required to complete for each system, agency systems may still not be secure. This CISO went on to say that his agency often must decide between using funding to fulfill compliance requirements versus using it in a way he feels would increase cyber resilience.

The order requires all federal government agencies to develop a plan to implement zero trust architecture according to NIST guidance, and to provide a planned schedule for implementing it. Due to its

⁵⁵Continuing resolutions are temporary spending bills that allow federal government operations to continue when final appropriations have not been approved by Congress and the President. Without final appropriations or a continuing resolution, there could be a lapse in funding that results in a government shutdown.

architecture, implementing zero trust architecture would enable more resilient agency networks.

Conclusions

Agencies have implemented a majority of the leadership and oversight requirements in Executive Order 14028, to enable greater protection of federal government networks against cybersecurity threats. However, implementation of the remaining outstanding requirements is also essential to improving the overall cyber resilience of the federal government. Fully clarifying which software categories are considered critical to agency operations would enhance the oversight that agencies are able to conduct on their software vendors. Further, documenting details of the resourcing support provided to agencies to improve their detection and remediation of cyber vulnerabilities and incidents could provide greater assurance that agencies will have the funding they need to implement these requirements.

Recommendations for Executive Action

We are making a total of five recommendations; two to the Department of Homeland Security and three to OMB. Specifically:

The Secretary of Homeland Security should direct the Director of CISA to issue, in a timely manner, its list of software and software product categories that are considered critical software. (Recommendation 1)

The Secretary of Homeland Security, through the Director of the CISA, should direct the Cyber Safety Review Board to document steps taken or planned to implement the recommendations provided to the President for improving the board's operations. (Recommendation 2)

The Director of OMB should demonstrate that the office has conducted, with pertinent federal agencies, cost analyses for the implementation of recommendations related to the sharing of threat information, as defined in the order. (Recommendation 3)

The Director of OMB should demonstrate that the office has coordinated with pertinent federal agencies regarding resourcing needs for the implementation of an endpoint detection and response capability, as defined in the order. (Recommendation 4)

The Director of OMB should demonstrate that the office has coordinated with pertinent federal agencies regarding resourcing needs for logging, log retention, and log management capabilities, as defined in the order. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to DHS and OMB, the agencies to which we made recommendations. We also provided a draft for comment to the Department of Commerce and ONCD.

- In written comments, DHS, through CISA, agreed with two of our recommendations, but disagreed with a third originally included in our draft report. Specifically, DHS agreed with our recommendation to issue a list of critical software, and they plan to make this list available to federal agencies by September 30, 2024. In addition, it agreed with

our recommendation to direct the Cyber Safety Review Board to document steps taken or planned to implement the recommendations provided to the President for improving the board's operations. According to DHS, the board has already begun to take steps to implement this recommendation, such as appointing the ONCD Director as a member of the board. DHS plans to establish a process for documenting additional steps necessary to fully implement this recommendation by December 31, 2024.

DHS disagreed with our recommendation included in a draft of this report to direct the Cyber Safety Review Board to conduct a review into the December 2020 SolarWinds cyber incident as required by Executive Order 14028. DHS stated that the board incorporated some aspects of the independent analysis conducted on SolarWinds into its Log4j review. In addition to DHS's response to our draft, we obtained additional information on actions taken by the federal government to review the SolarWinds incident. Upon further review of DHS' comments and the additional information obtained, we agree that the federal government had taken sufficient steps to review the SolarWinds incident. Therefore, we removed our related finding and withdrew the recommendation from the final report. DHS's comments are reproduced in appendix IV.

- In an email, an official in OMB's Office of General Counsel stated that the office had no comments or response on the report.
- In an email, ONCD's General Counsel stated that the office did not have any comments on the report.

DHS and the Department of Commerce, through NIST, also provided technical comments, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Director of CISA, the Director of OMB, the National Cyber Director, the Secretary of Homeland Security, 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 Marisol Cruz Cain at (202) 512-5017 or cruzcainm@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 V.

Letter

A handwritten signature in black ink that reads "Marisol Cruz Cain". The signature is written in a cursive style with a distinct dot over the 'i' in "Cruz".

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine to what extent (1) agencies have implemented the leadership and oversight-related requirements in Executive Order 14028, and (2) the order has addressed federal cybersecurity challenges.

For our first objective, we identified 115 provisions of Executive Order 14028.¹ We then identified a subset of provisions that required an action with government-wide leadership or oversight focus. Among other things, this included provisions that were (1) contextual and did not contain any action, (2) related to only a small subset of systems, or (3) that required actions on the part of each individual agency regarding their own systems. Also, if the actions taken in two provisions were dependent on each other, we considered them as one combined requirement. As a result of these steps, we narrowed our focus to 55 leadership and oversight requirements.

We then selected a subset of four agencies that perform leadership and oversight actions in implementing the order. Specifically, we selected the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA); the National Institute of Standards and Technology (NIST); the Office of Management and Budget (OMB); and the Office of the National Cyber Director (ONCD). We selected CISA, NIST, and OMB based on the significant number of the order's requirements assigned to them, as well as the government-wide leadership and oversight nature of the requirements assigned to them. We selected ONCD because, in early 2022, it took on overall responsibility over the order's implementation.²

We next determined a key owner for each of the 55 requirements from among the leadership and oversight agencies. In most cases, this was the agency assigned the key responsibility in the text of the order. In other

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

²When the order was developed in May 2021, it included a provision to allow some of its responsibilities to be transferred to ONCD once it was established. Subsequently, in early 2022, ONCD took on its current oversight responsibility over the order's implementation.

cases, such as when the order assigned a provision to more than one agency, we assigned a key owner based on context. Context factors included the owner of other related requirements, or clarification from agencies on which of them were leading implementation of a requirement's actions. For each of the 55 requirements, we summarized its language to remove jargon, repetitive language, or unclear linkages that might prevent a reader from understanding its contents.

We then analyzed the extent to which each of the 55 requirements have been completed, based on artifacts such as guidance, memoranda, interviews with relevant agency officials, reports, and contract language. We split the requirements into seven sections based on the sections in the order that contained at least one leadership and oversight requirement.³ We assessed 54 of the 55 requirements on a three-point scale. Possible assessments for each requirement were fully complete, partially complete, not complete, or not applicable.

- Fully completed requirements were those where the actions required are complete.
- Partially completed requirements were those where we assessed significant progress to be made in completing a requirement.
- Requirements considered not complete were those where the progress made toward completion was minimal and not significant.

We also considered one requirement's score not applicable due to timing conditions that prevented its actions from being performed during the time of our review.

For our second objective, we used information from GAO's High-Risk Series reports to identify a list of 10 federal cybersecurity critical actions. We then conducted a small group discussion with six federal chief information security officers (CISO), which were identified by the CISO Council as having relevant experience regarding the order and were able to participate in the discussion. At this discussion, we determined CISOs' perspectives on the 10 identified critical actions, and the extent to which CISOs found taking these actions to be challenging in their day-to-day operations. CISOs also identified three broader issues that they consider

³Eight of the order's 11 sections contain required actions for federal agencies to perform toward achieving a specific cybersecurity goal, with the other three sections supplying context and supporting information. Of the eight sections with required actions, we found that seven sections contained leadership and oversight requirements.

to be challenges for their agencies' cyber operations. Of the action areas and issues discussed, these CISOs also identified three areas they found most challenging overall.

We then analyzed which of the action areas and issues are addressed by the order. Specifically, we compared the 10 cyber action areas listed in GAO's High-Risk report, as well as the three broader issues mentioned by CISOs, against the order's requirements. For any areas not addressed by the order, we considered whether other recently issued government frameworks, strategies, or guidance were likely to address them.

We conducted this performance audit from October 2022 to April 2024 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: Responsibilities in Executive Order 14028

The following table lists all provisions, by section, in Executive Order 14028.¹

Table 10: Provisions and Agencies Responsible in Executive Order 14028

Section number	Agencies	Provision(s)
<p>Section 1: Policy – The federal government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include IT systems that process data and those that run the vital machinery that ensures our safety (operational technology). The prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. All federal information systems should meet or exceed the standards and requirements for cybersecurity set forth and issued in this order.</p>		
<p>Section 2: Removing Barriers to Sharing Threat Information – This section includes removing contractual barriers and increasing the sharing of information about threats, incidents, and risks. These are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies’ systems and of information collected, processed, and maintained by or for the federal government.</p>		
2b	Office of Management and Budget (OMB) in consultation with the Department of Defense (DOD), Attorney General, Department of Homeland Security (DHS), and Office of the Director of National Intelligence	Review the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and operational technology service providers and recommend updates to such requirements and language to the Federal Acquisition Regulatory Council
2c		Design recommended contract language and requirements described in subsection (b) to ensure that service providers:
2c(i)	OMB in consultation with DOD, Attorney General, DHS, and Office of the Director of National Intelligence	collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies’ requirements
2c(ii)		share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted
2c(iii)	OMB in consultation with DOD, Attorney General, DHS, and Office of the Director of National Intelligence	collaborate with federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on federal information systems, including implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed
2c(iv)		share cyber threat and incident information with agencies, and do so, where possible, in industry-recognized formats for incident response and remediation

¹As described in appendix I, some leadership and oversight provisions that were dependent on each other were combined and considered as one requirement as part of the 55 total leadership and oversight requirements used in this report.

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
2d	Federal Acquisition Regulatory Council	Review and publish the recommendations for public comment and propose updates to the Federal Acquisition Regulation
2e	DHS and OMB	Take steps to ensure that service providers share data on cyber threats, incidents, and risks, to the greatest extent possible
2f	Not Applicable	Federal government policy states that the following actors take the following actions:
2f(i)	Information and communications technology service providers	Report to agencies promptly when a cyber incident involving a software product or a support system provided to such agencies is discovered
2f(ii)	Information and communications technology service providers Cybersecurity and Infrastructure Security Agency (CISA)	Report to CISA when discovering a cyber incident involving a support system for a software product or service provided to such agencies Centrally collect and manage such information
2f(iii)	Federal civilian executive branch agencies	Receive and manage reports pertaining to national security systems, as applicable and as determined by national security systems reporting requirements
2g	Not Applicable	To implement the policy set forth in subsection (f) of this section:
2g(i)	DHS	Recommend contract language on the nature of cyber incidents requiring reporting, the types of information on incidents that will facilitate response and remediation, appropriate and effective protections for privacy and civil liberties, time periods for acceptable reporting by contractors, reporting requirements for national security systems, and types of contractors and service providers covered by the proposed contract language
2g(ii)	Federal Acquisition Regulatory Council	Review and publish proposed updates to the Federal Acquisition Regulatory Council for public comment after receipt of the recommendations described in subsection g(i) of this section
2g(iii)	DOD, National Security Agency (NSA), Department of Justice, DHS, and the Office of the Director of National Intelligence	Develop procedures for ensuring that cyber incident reports are shared appropriately
2h	No agency is required to take action as a result of this provision	Standardize common cybersecurity contractual requirements across agencies to streamline and improve compliance for vendors and the federal government
2i	CISA in consultation with NSA, OMB, and the Administrator of General Services	Review agency-specific cyber requirements that currently exist and recommend standardized contract language, including scope of contractors and service providers covered by the proposed contract language
2j	Federal Acquisition Regulatory Council	Review and publish proposed updates to the Federal Acquisition Regulatory Council for public comment after receipt of the recommendations described in subsection (i) of this section
2k	Federal agencies	Update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of Federal Acquisition Regulation updates
2l	OMB	Incorporate into the annual budget process a cost analysis of the steps to be taken in this section

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
Section 3: Modernizing Federal Government Cybersecurity – The federal government must adopt security best practices; advance toward implementation of zero trust architecture; accelerate movement to secure cloud services; centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.		
3b	Not Applicable	The head of each agency shall:
3b(i)	Federal agencies	Update existing agency plans to prioritize resources for the adoption and use of cloud technology outlined in relevant OMB guidance
3b(ii)	Federal agencies	Develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) has outlined in standards and guidance
3b(iii)	Federal agencies OMB	Provide OMB and the Assistant to the President and National Security Advisor with plans to implement Zero Trust Architecture and to prioritize resources for adoption and use of technology Receive this information from all federal agencies
3c	Not Applicable	As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the federal government to prevent, detect, assess, and remediate cyber incidents. To facilitate this work:
3c(i)	OMB in consultation with CISA and General Services Administration Federal Risk and Authorization Management Program	Provide guidance to agencies to facilitate their implementation of zero trust architecture and ensure that risk from using cloud-based services is broadly understood and effectively addressed
3c(ii)	CISA in consultation with OMB and General Services Administration Federal Risk and Authorization Management Program	Develop and issue for agencies cloud security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting
3c(iii)	CISA	Develop a cloud-service governance framework that identifies a range of services and protections available to agencies based on incident severity, as well as data and processing activities associated with those services and protections
3c(iv)	Federal civilian executive branch agencies in consultation with CISA	Provide evaluation reports on the types and sensitivity of unclassified data, including identification of the unclassified data considered to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data
3d	Federal civilian executive branch agencies	Adopt multifactor authentication and encryption for data at rest and in transit to the maximum extent consistent with federal records laws and other applicable laws
3d(i)	Federal civilian executive branch agencies	Provide reports every 60 days after the date of the order on agency progress in implementing multifactor authentication and data encryption until the agency has fully adopted them agencywide
3d(ii)	CISA	Take appropriate steps to maximize adoption by federal civilian executive branch agencies of multifactor authentication and encryption for data at rest and in transit based on identified gaps
3d(iii)	Federal civilian executive branch agencies	Provide a written rationale if unable to fully adopt multifactor authentication and data encryption within the prescribed date

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
3e	CISA in consultation with the Department of Justice, the Federal Bureau of Investigation, and the General Services Administration Federal Risk and Authorization Management Program	Establish a framework to collaborate on cybersecurity and incident response activities related to cloud technology to ensure effective information sharing among agencies and between agencies and cloud service providers
3f(i-v)	General Services Administration in consultation with OMB and federal agencies	Modernize the Federal Risk and Authorization Management Program by, among other things, establishing an effective training program, improving communication with service providers, incorporating automation, streamlining vendor documentation, and identifying relevant compliance frameworks
Section 4: Enhancing Software Supply Chain Security - The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The federal government must take action to rapidly improve the security and integrity of the software supply chain.		
4b	NIST	Solicit input from the federal government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools and best practices that enhance the security of the software supply chain
4c	NIST	Publish preliminary guidelines for enhancing software supply chain security based on consultation and drawing on existing documents as practicable
4d	NIST	Update guidelines and publish additional procedures for periodic review for enhancing software supply chain security
4e(i-x)	NIST	Issue guidance identifying practices that enhance the security of the software supply chain. Guidance shall identify standards, procedures, and criteria regarding secure software development environments; employ automated tools, or comparable processes, to maintain trusted source code supply chains, employ automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them; and maintain accurate and up-to-date data and origins of software code or components.
4f	Department of Commerce and the National Telecommunications and Information Administration	Publish elements for a software bill of materials ^a
4g	NIST in consultation with DOD, OMB, and the Office of the Director of National Intelligence	Publish definition of the term “critical software” for inclusion in the guidance for enhancing the security of the software supply chain
4h	CISA in consultation with NIST	Identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of “critical software”
4i	NIST in consultation with CISA and OMB	Publish guidance outlining security measures for critical software, including applying practices of least privilege, network segmentation, and proper configuration
4j	OMB	Require agencies to comply with guidance described in subsection (i) of this section
4k	OMB	Require agencies to comply with such guidelines with respect to software procured after the date on which the order was issued

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
4l	Federal agencies OMB	Request an extension for compliance with any requirements issued pursuant to subsection (k) of this section on a case-by-case basis, accompanied by a plan for meeting the underlying requirements. Provide, on a quarterly basis, a report to the Assistant to the President for National Security Affairs identifying and explaining all extensions granted.
4m	Federal agencies OMB, in consultation with the Assistant to the President for National Security Affairs	Request a waiver for compliance with any requirements issued pursuant to subsection (k) of this section. Consider waivers on a case-by-case basis. Waivers are granted only in exceptional circumstances and for a limited duration.
4n	DHS in consultation with DOD, OMB, and the Attorney General	Recommend to the Federal Acquisition Regulatory Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, guidance that enhances the security of the software supply chain
4o	Federal Acquisition Regulatory Council	Review the recommendations described in subsection (n) of this section, and, as appropriate and consistent with applicable law, amend the Federal Acquisition Regulation
4p	Federal agencies	Remove software products that do not meet the requirements of the amended Federal Acquisition Regulation described in subsection (o) from specified contract types following the issuance of any final rule amending the Federal Acquisition Regulation
4q	OMB	Require agencies employing software developed and procured prior to the issue date of Executive Order 14028, known as legacy software, to either comply with any requirements issued in response to subsection (k) of this section, or to provide a plan outlining action to remediate or meet those requirements
4r	NIST	Publish guidelines recommending minimum standards for vendor testing of software source code
4s	NIST	Initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet of Things devices and software development practices and consider ways to incentivize manufacturers and developers to participate in these programs
4t	NIST	Identify Internet of Things cybersecurity criteria for a consumer labeling program, and consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law
4u	NIST	Identify secure software development practices or criteria for consumer software labeling programs and consider whether a consumer software labeling program may be operated in conjunction with or modeled after any similar government programs, consistent with applicable law
4v	NIST	Conduct the pilot programs described in subsection (s) of this section in a manner consistent with guidance on conformity assessments
4w	NIST	Conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, and determine what improvements can be made going forward. Submit a summary report to Assistant to the President for National Security Affairs.
4x	Department of Commerce	Provide the President, through the Assistant to the President for National Security Affairs, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
Section 5: Establishing a Cyber Safety Review Board – The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board.		
5a	DHS	Establish the Cyber Safety Review Board, pursuant to section 871 of the Homeland Security Act of 2002
5b	Cyber Safety Review Board	Convene the board to review and assess significant cyber incidents affecting federal civilian executive branch information systems or non-federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses
5c	DHS	Convene the board following a significant cyber incident triggering the establishment of a cyber unified coordination group, when the President directs, or when the Secretary of Homeland Security deems necessary
5d	Cyber Safety Review Board	Conduct an initial review related to the cyber activities that prompted the establishment of a cyber unified coordination group in December 2020, and provide recommendations to DHS for improving cybersecurity and incident response practices
5e	DHS	Ensure that the board’s membership shall include federal officials and representatives from private-sector entities
5f	DHS	Designate a chair and deputy chair of the board biennially from among the members of the board, to include one federal and one private-sector member
5g	Cyber Safety Review Board	Protect sensitive law enforcement, operational, business, and other confidential information that has been shared with the board consistent with applicable law
5h	DHS	Provide to the President through the Assistant to the President for National Security Affairs, any advice, information, or recommendations of the board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident
5i (i-v)	DHS	Provide the President with recommendations for improving the board’s operations such as: identifying gaps in and options for the board’s composition or authorities; membership eligibility criteria for private sector representatives; and administrative and budgetary considerations required for operation of the board
5j	DHS	Review the recommendations provided to the President through the Assistant to the President for National Security Affairs in subsection (i) of this section and take steps to implement them as appropriate
5k	DHS	Unless otherwise directed by the President, extend the life of the board every 2 years as the Secretary of Homeland Security deems appropriate, pursuant to section 871 of the Homeland Security Act of 2002
Section 6: Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents – This section includes development of standardized cybersecurity vulnerability and incident response processes to ensure a more coordinated and centralized cataloging of incidents and tracking of agencies’ progress toward successful responses.		
6b(i-iii)	CISA in consultation with OMB and others, and in coordination with DOD, the Department of Justice, and the Director of National Intelligence	Develop a standard set of operational procedures, or playbook, to be used in planning and conducting a cybersecurity vulnerability and incident response activity to be used by federal civilian executive branch agencies. The playbook shall incorporate NIST standards and articulate progress and completion through all phases of an incident response while allowing flexibility in support of various response activities.
6c	OMB	Issue guidance to agencies on use of the playbook

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
6d	Federal civilian executive branch agencies in consultation with OMB and the Assistant to the President for National Security Affairs	Ensure that agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook may use such procedures only after consulting with the Director of OMB and the Assistant to the President for National Security Affairs and demonstrating that these procedures meet or exceed the standards proposed in the playbook
6e	CISA in consultation with NSA	Review and update the playbook annually and provide information to OMB to incorporate in guidance updates
6f	CISA	Establish a requirement to review and validate agencies' incident response and remediation results upon an agency's completion of incident response activities
6g	CISA	Define key cybersecurity terms in the playbook and use such terms consistently with any statutory definitions of those terms, to the extent practicable
Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks – The federal government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks.		
7b	Federal civilian executive branch agencies	Implement endpoint detection and response (EDR) initiative to support proactive definition of cyber incidents
7c	DHS	Provide recommendations to OMB on options for implementing an EDR initiative, centrally located to support host-level visibility, attribution, and response regarding federal civilian executive branch information systems
7d	OMB in consultation with DHS	Issue requirements for federal civilian executive branch agencies to adopt EDR approaches, including supporting a capability for CISA to engage in cyber hunt, detection, and response activities
7e	OMB	Work with DHS and agency heads to ensure that agencies have adequate resources to comply with the requirements issued in this section regarding the adoption of EDR approaches
7f	Federal civilian executive branch agencies with CISA	Establish or update memoranda of agreement with CISA to ensure that needed data are available and accessible to CISA's Continuous Diagnostics and Mitigation program
7g	NSA	Recommend actions for improving detection of cyber incidents affecting national security systems including recommendations concerning EDR approaches
7h	DOD, Office of the Director of National Intelligence, and Committee on National Security Systems	Review the recommendations submitted under subsection (g) of this section and, establish policies that effectuate those recommendations
7i	CISA	Provide OMB and the Assistant to the President for National Security Affairs a report describing how authorities to conduct threat-hunting activities on federal civilian executive branch networks without prior authorization from agencies are being implemented. This report should include procedures to ensure that mission-critical systems are not disrupted, procedures for notifying system owners of vulnerable government systems, and the range of techniques that can be used during test of federal civilian executive branch information systems.
7j	Not Applicable	To ensure alignment between Department of Defense Information Network directives and federal civilian executive branch information systems directives:

Appendix II: Responsibilities in Executive Order 14028

Section number	Agencies	Provision(s)
7j(i)	DOD and DHS in consultation with OMB	Establish procedures for DOD and DHS to immediately share DOD incident response orders or DHS Emergency Directives and Binding Operational Directives applying to their respective information networks
7j(ii)	DOD and DHS in consultation with OMB	Evaluate whether to adopt any guidance contained in an order or directive issued by DOD or DHS, consistent with regulations concerning sharing of classified information
7j(iii)	DOD and DHS in consultation with OMB	Notify the Assistant to the President for National Security Affairs and OMB of the evaluation within seven days of receiving notice of an order or directive issued consistent with the procedures in this section, including a determination whether to adopt guidance issued by the other department, the rationale for the determination, and a timeline for application of the directive
Section 8: Improving the Federal Government's Investigative and Remediation Capabilities – This section includes actions to improve access to information from network and system logs on federal information systems, for both on-premises systems and connections hosted by third parties, such as cloud service providers.		
8b	DHS in consultation with the Attorney General and OMB	Provide OMB with recommendations on requirements for logging events and retaining other relevant data within an agency's systems and networks, including on the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs
8c	OMB in consultation with Commerce and DHS	Formulate policies for agencies to establish requirements for logging, log retention, and log management, to ensure centralized access and visibility for the highest-level security operations center of each agency
8d	OMB	Work with agency heads to ensure that agencies have adequate resources to comply with requirements in this section for logging, log retention, and log management
8e	DHS in consultation with the Attorney General and OMB Federal agencies	Include within the recommendations developed in this section requirements for sharing logs related to cyber risks or incidents Provide logs that meet the requirements in this section to CISA and the Federal Bureau of Investigation
Section 9: National Security Systems		
9a	DOD in coordination with the Office of the Director of National Intelligence and Committee on National Security Systems	Adopt all requirements in the order pertaining to national security systems, and codify them in a national security memorandum
9b	No agency is required to take action as a result of this requirement	Nothing in Executive Order 14028 shall alter the authority of the National Manager with respect to national security systems as defined in National Security Directive 42 of July 5, 1990. The federal civilian executive branch agencies network shall continue to be within the authority of the Secretary of Homeland Security acting through the Director of CISA.

Section 10: Definitions – Defined key terms, concepts, and entities for the purpose of this order.

- a) The term “agency” means any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, as defined in 44 U.S.C. § 3502(5).
- b) The term “auditing trust relationship” means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.
- c) The term “cyber incident” means an occurrence that jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system. Furthermore, it constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies, as defined in 44 U.S.C. § 3552(b)(2) under “incident”.
- d) The term “Federal Civilian Executive Branch Agencies” or “FCEB Agencies” includes all agencies except for the Department of Defense and agencies in the intelligence community.
- e) The term “Federal Civilian Executive Branch Information Systems” or “FCEB Information Systems” means those information systems operated by Federal Civilian Executive Branch Agencies excluding national security systems.
- f) The term “Federal Information Systems” means an information system used or operated by an agency, a contractor of an agency or by another organization on behalf of an agency, including FCEB Information Systems and national security systems.
- g) The term “intelligence community” includes the following: Office of the Director of National Intelligence, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs, the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Department of Energy, Bureau of Intelligence and Research of the Department of State, Office of Intelligence and Analysis of the Department of the Treasury, and the Office of Intelligence and Analysis of the Department of Homeland Security, or such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as defined in 50 U.S.C. 3003(4).
- h) The term “National Security Systems” means any information system used or operated by an agency, a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves the following: intelligence activities; cryptologic activities related to national security; command, control and equipment of military forces and weapon systems or is critical to the direct fulfillment of military or intelligence missions; or specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy, as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3).
- i) The term “logs” means records of the events occurring within an organization’s systems and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.
- j) The term “Software Bill of Materials” or “SBOM” means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.
- k) The term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

Section 11: General Provisions

- a) Upon the appointment of the National Cyber Director and the establishment of the related office within the Executive Office of the President, pursuant to section 1752 of Public Law 116-283, portions of this order may be modified to enable the National Cyber Director to fully execute its duties and responsibilities.
- b) Nothing in this order shall be construed to impair or affect: the authority granted by law to an executive department or agency, or the head thereof; or the functions of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.
- c) The order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.
- d) The order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Nothing in this order confers authority to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned during a criminal or national security investigation.

Source: GAO analysis of information in Executive Order 14028. | GAO-24-106343

Note: As described in appendix I, some leadership and oversight provisions that were dependent on each other were combined and considered as one requirement as part of the 55 total leadership and oversight requirements used in this report.

^aAn [Software Bill of Materials] SBOM is effectively a nested inventory, a list of ingredients that make up software components. An SBOM identifies and lists software components, information about those components, and supply chain relationships between them. See National Telecommunications and Information Administration, *Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)*, (October 21, 2021).

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

The following table summarizes the progress agencies have made in implementing the 55 leadership and oversight requirements in the order.

Table 11: Status and Details of Leadership and Oversight Requirements in Executive Order 14028, as of March 2024

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Review contract requirements for service providers and recommend updates to requirements and language in the contracts	CISA	Fully implemented	CISA submitted contract clauses and recommendations that emphasized a government-wide approach to sharing cyber incident information to the Federal Acquisition Regulatory Council for review. In October 2023, the council published a proposed rule based on the information in these contract clauses.
Recommend contract language on the nature of cyber incidents requiring reporting	CISA	Fully implemented	
Ensure that service providers share data on cyber threats, incidents, and risks, to the greatest extent possible	CISA/OMB	Fully implemented	CISA and OMB took steps to ensure that service providers share needed data on cyber threats, incidents, and risks. For example, in September 2021, CISA and OMB issued a joint statement that a major service provider would share its information on cyber incidents and threat actors with federal agencies.
Manage information reported by agency-contracted service providers when they discover a cyber incident involving a product or service provided to an agency	CISA	Fully implemented	CISA, through its Automated Indicator Sharing service, provides real-time exchange of machine-readable cyber indicators and defense measures between the public and private sectors. CISA also provides additional resources for online reporting including an incident reporting page and the folder of which shows how they manage and collect cyber incidents.
Develop, with input from other agencies, procedures for ensuring that cyber incident reports are shared among agencies	CISA	Fully implemented	CISA developed procedures to help ensure that cyber incident reports developed by service providers are shared among agencies. Among other things, these procedures identified information that CISA must receive from service providers and share with its federal partners, and the timeframes in which CISA should share this information.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Review agency-specific cyber requirements that exist and recommend standardized contract language	CISA	Fully implemented	CISA received over 600 detailed agency-specific cybersecurity contract requirements from chief information officers and chief information security officers and, in consultation with other agencies, made recommendations related to them.
Incorporate into annual budget process a cost analysis of the steps to be taken in this section	OMB	Partially implemented	OMB issued a memorandum outlining cybersecurity budget priorities, and, according to staff, held regular communications with agencies on implementing these priorities. However, OMB did not provide evidence that it had incorporated an analysis of specific costs agencies would incur in implementing recommendations for sharing cyber threat information.
Modernizing Federal Government Cybersecurity			
Receive information from agencies regarding their plans to implement zero trust architecture	OMB	Fully implemented	OMB and CISA received and subsequently reviewed zero trust architecture implementation plans from 70 agencies. OMB and CISA also held guidance sessions to ensure that agencies took steps toward implementing their plans, including assessing their cyber environments in preparation for the implementation, and ensuring they understood the resources needed.
Provide guidance to agencies that move closer to implementing zero trust architecture and ensure that the risk from using cloud-based services is addressed	OMB	Fully implemented	OMB issued a memorandum which set up specific cybersecurity standards for implementing zero trust architecture.
Develop and issue for agencies a cloud security technical reference architecture documentation	CISA	Fully implemented	CISA developed and issued a cloud security technical reference architecture for agencies that recommends approaches on cloud migration and data protection for agency data collection and reporting.
Develop a cloud-service governance framework that identifies a range of services and protections available to agencies based on incident severity, as well as data and processing activities	CISA	Fully implemented	CISA submitted a cloud-service governance framework to OMB. In it, CISA recommends adoption of a threat-based risk management model that focuses on identifying and prioritizing countermeasures against all phases of a cyber intrusion.
Receive evaluation reports from agencies on the types and sensitivity of their respective unclassified data	CISA	Fully implemented	CISA established a template for agencies to provide the agency with information on the type, sensitivity, and other attributes regarding data on agency systems. CISA receives reports from agencies with this information through a secure automated system.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Receive reports from agencies on progress in adopting multifactor authentication and encryption of data at rest and in-transit, and take all appropriate steps to maximize adoption by agencies	CISA	Fully implemented	CISA managed agencies' progress in adopting multifactor authentication and encryption of data at rest and in-transit through metrics developed under the Federal Information Security Modernization Act of 2014. The metrics have been updated to reflect the reporting requirements outlined in the order.
Receive a written rationale from all agencies that are unable to fully adopt multifactor authentication and data encryption within the prescribed date	CISA	Fully implemented	CISA requires any agency unable to fully adopt multifactor authentication and encryption to certify a risk acceptance. As part of the risk acceptance process, agencies must report the remaining gaps and priorities to sustain improvement in implementation of these requirements.
Establish a framework to collaborate on cybersecurity and incident response activities related to cloud technology	CISA	Fully implemented	CISA developed a framework to collaborate on incident response activities as part of its technical reference architecture. The framework required that agencies follow established government-wide incident and communication procedures when reporting cybersecurity incidents.
Enhancing Software Supply Chain Security			
Solicit input and publish preliminary guidelines to enhance the security of the software supply chain	NIST	Fully implemented	NIST solicited input for these guidelines by conducting a workshop with over 1,000 participants and reviewing over 150 position papers. It then published and updated guidelines on identifying, assessing, and mitigating supply chain risks.
Update guidelines and publish additional procedures for periodic review to enhance software supply chain security	NIST	Fully implemented	
Issue guidance identifying practices that enhance the security of the software supply chain. Guidance shall identify standards, procedures, and criteria such as establishing multifactor, risk-based authentication.	NIST	Fully implemented	NIST published a secure software development framework which contained standards, procedures, and criteria for mitigating the risk of software vulnerabilities. NIST also published recommended supply chain risk management practices for systems and organizations.
Publish the definition of the term "critical software"	NIST	Fully implemented	NIST published a definition for critical software based on the input it received from the workshop and position papers mentioned above. It also consulted with CISA, OMB, and other agencies to develop the definition.
Identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of "critical software"	CISA	Partially implemented	CISA, OMB, and NIST developed a definition of critical software and a preliminary list of common categories of software that are consistent with the definition developed by NIST. However, CISA has not issued the list.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Publish guidance outlining security measures for “critical software”	NIST	Fully implemented	NIST published guidance outlining security measures for critical software. Among other things, NIST identified key practices such as defining key performance indicators and other criteria for determining software security, segregating software development environments, and making integrity verification information available to those responsible for software acquisition.
Require agencies to comply with guidance outlining security measures for “critical software”	OMB	Fully implemented	OMB issued a memorandum instructing agencies on the use of secure software development practices to secure their supply chains. This memorandum instructed agencies on actions and timelines for steps to secure their supply chain according to the NIST guidelines, including for legacy software.
Require agencies to comply with guidelines for enhancing the security of the software supply chain for software procured after the date of Executive Order 14028	OMB	Fully implemented	OMB issued a memorandum with requirements for agencies with respect to the security of agencies’ software supply chain, including the procuring of self-attestations on software practices, and the development of consistent practices for vendors to follow. In March 2024, CISA and OMB issued a software development attestation form to further guide agencies on required actions in this area.
Identify and explain all extensions or waivers granted to agencies for not complying with requirements to enhance software supply chain security for all software procured after the date of the order and report these on a quarterly basis	OMB	Fully implemented	OMB issued a memorandum which included specific instructions to agencies on requesting extensions or waivers to the software supply chain requirements listed in the memorandum. Due to subsequent guidance by OMB, the deadline by which agencies must submit extensions or waivers has not yet passed, and no extensions or waivers have yet been submitted.
Recommend to the Federal Acquisition Regulatory Council contract language requiring suppliers of software available for purchase by agencies to comply with guidance that enhances the security of the software supply chain	CISA	Fully implemented	CISA drafted contract language that contained requirements for the development of IT software designated as critical software. Among other things, requirements included following NIST guidance for secure software development and use of critical software.
Require agencies employing software developed and procured prior to Executive Order 14028, including legacy software, to provide a plan outlining action to remediate or meet those requirements issued in this section	OMB	Fully implemented	OMB issued a memorandum clarifying that requirements to agencies regarding securing their software supply chain also applied to software developed prior to its issuance. In this memorandum, OMB required agencies to submit plans for remediating any issues with software providers by June 2024.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Publish guidelines recommending minimum standards for vendor testing of software source code	NIST	Fully implemented	NIST made recommendations for software verification techniques such as threat modeling and use of built-in test cases. NIST also provided references with supplemental information about the techniques.
Initiate pilot programs, consistent with existing guidance and informed by existing consumer product labeling programs, to educate the public on the security capabilities of Internet of Things devices and software development practices	NIST	Fully implemented	NIST initiated pilot programs regarding labeling efforts for consumer Internet of Things products and consumer software. As part of the pilots, NIST engaged with federal agency experts through public comments and workshops to develop criteria for a labeling program.
Identify Internet of Things cybersecurity criteria for a consumer labeling program, and consider whether a consumer labeling program may be operated in conjunction with or modeled after any similar government programs	NIST	Fully implemented	NIST made recommendations for consumer Internet of Things product label criteria, including label design and consumer education considerations.
Identify secure software development practices or criteria for a consumer software labeling program and consider whether a consumer software labeling program may be operated in conjunction with or modeled after any similar government programs	NIST	Fully implemented	NIST made recommendations for baseline technical criteria for the information that can appear on a software label and labeling presentation criteria.
Conduct a review of the pilot programs and submit a summary report to the Assistant to the President for National Security Affairs	NIST	Fully implemented	NIST performed a summary review of the effectiveness of the cybersecurity labeling pilot programs, and issued a report based on this review to the Assistant to the President for National Security Affairs.
Provide the President, through the Assistant to the President for National Security Affairs, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain	NIST	Fully implemented	NIST issued a report that provided a summary of the work it performed for each of the responsibilities assigned to it in the software supply chain security section of the order.
Establishing a Cyber Safety Review Board			

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Establish a Cyber Safety Review Board (board) comprised of representatives from the federal government and private-sector cybersecurity or software suppliers. Biennially extend the life of the board and designate a Chair and Deputy Chair unless otherwise directed by the President.	CISA	Fully implemented	The Department of Homeland Security, through CISA, established the Cyber Safety Review Board. The board is comprised of representatives from the private sector and federal government.
Convene the board to review and assess significant cyber incidents affecting federal civilian executive branch information systems or non-federal systems	CISA	Fully implemented	The board completed its first incident review—the Log4j event that occurred in December 2021. ^a The board subsequently conducted a second review of the Lapsus\$ threat actor group. ^b
Convene the board to perform an initial review that shall relate to the cyber activities that prompted the establishment of a Cyber Unified Coordination Group in December 2020. ^c The board shall provide recommendations to the Department of Homeland Security for improving cybersecurity and incident response practices based on this review.	CISA	Fully implemented	The federal government performed a review of the cyber activities related to the December 2020 SolarWinds incident. This review included a timeline of events, details on the vulnerability that was exploited, agency responses, and mitigation activities. In addition, the board provided a report to the Department of Homeland Security for improving cybersecurity and incident response practices based on the Log4j review, which included information on the SolarWinds review.
Confirm that the board protects sensitive law enforcement, operational, business, and other confidential information that has been shared with it	CISA	Fully implemented	The board’s charter requires it to protect sensitive law enforcement, operational, business, and other confidential information, consistent with applicable law. Reports may also include an annex with classified material and other sensitive nonpublic information that is protected from public release.
Provide the President with any advice, information, or recommendations of the board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident	CISA	Fully implemented	Both the Log4j ^a and Lapsus\$ ^b incident reviews completed by the board contained recommendations, in areas such as coordinating information on risks and adopting industry-accepted practices for access management and vulnerability management.
Provide the President with recommendations for improving the board’s operations	CISA	Fully implemented	The board reviewed its operations and provided recommendations for improvement in areas such as establishing methods for the collection of information and establishing practices regarding access to and handling of classified information.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Review the recommendations provided to the President for improving the board's operations and take steps to implement them as appropriate	CISA	Partially implemented	CISA officials stated that it has made progress in implementing the board's recommendations and is planning further steps to improve the board's operational policies and procedures. However, CISA has not provided evidence that it is implementing the recommendations made by the board to improve its future operations.
Standardizing a Playbook for Responding to Cybersecurity Vulnerabilities and Incidents			
Develop a standard set of operational procedures, or playbook, to be used in planning and conducting a cybersecurity vulnerability and incident response activity to be used by agencies. To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms.	CISA	Fully implemented	CISA published a playbook that provides operational procedures for agencies to use in planning and conducting cybersecurity vulnerability and incident response activities.
Issue guidance to agencies on use of the playbook	OMB	Fully implemented	OMB issued to agencies a memorandum with required steps for implementing the playbook.
Consult with agencies on any deviations from the playbook and require them to demonstrate that any deviations meet or exceed the standards proposed in the playbook	OMB	Not Applicable	OMB was not able implement the order's requirement to consult with agencies on deviations from the playbook because no agencies have requested deviations. Since the order focuses only on actions resulting from a deviation request, no actions are required on the part of OMB, and this requirement is currently considered to be not applicable.
Review and update the playbook annually and provide information to OMB to incorporate in guidance updates	CISA	Fully implemented	CISA has reviewed the playbook annually and as a result, determined that no additional updates to the document were needed.
Establish a requirement to review and validate agencies' incident response and remediation results upon an agency's completion of incident response activities	CISA	Fully implemented	CISA included in the playbook a requirement for it to validate agency incident and vulnerability response results and processes. According to the playbook, validation assures agencies that they are meeting baseline standards, implementing all important steps, and have fully eradicated an incident or vulnerability.
Improving Detection of Cybersecurity Vulnerabilities and Incidents			
Provide recommendations to OMB on options for implementing an endpoint detection and response (EDR) initiative	CISA	Fully implemented	CISA provided OMB with recommendations on options for implementing an EDR initiative. Among the approaches suggested by CISA were the deployment of a commercial EDR solution across all agencies, and deployment of software focused on providing CISA with government-wide visibility and more rapid attribution of root causes for incidents that are detected.

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Issue requirements for agencies to adopt EDR approaches, including supporting a capability for CISA to engage in cyber hunt, detection, and response activities	OMB	Fully implemented	OMB issued guidance for agencies to follow in implementing EDR approaches, based on options provided by CISA. Specifically, the OMB guidance provided implementation steps for agencies as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the government.
Ensure that agencies have adequate resources to comply with the requirements for adopting EDR approaches	OMB	Partially implemented	CISA demonstrated it had worked with agencies to ensure they had adequate resources to implement EDR approaches. However, OMB could not demonstrate it had documented the results of communications with agencies to discuss agencies' resource concerns.
Establish or update Memoranda of Agreement with CISA for the Continuous Diagnostics and Mitigation (CDM) program to ensure that needed data, are available and accessible to CISA	CISA	Fully implemented	CISA had established memoranda of agreement with agencies to maintain access to the data needed to conduct its CDM program. Specifically, the memoranda identified CDM capabilities to be implemented at each agency, such as asset management, identity and access management, and network security management. It also defined the roles and responsibilities of both CISA and the agencies in implementing and operating CDM tools, sensors, and agency dashboards.
Provide OMB and the Assistant to the President for National Security Affairs a report describing how authorities to conduct threat-hunting activities on federal civilian executive branch agency networks without prior authorization from agencies are being implemented	CISA	Fully implemented	CISA submitted regular reports which highlighted its progress in three areas: proactively hunting for adversary activity on federal networks, proactively hunting for vulnerabilities on federal networks, and providing cybersecurity services to federal agencies.
Establish procedures for the Department of Defense (DOD) and Department of Homeland Security (DHS) to immediately share DOD incident response orders or DHS emergency directives and binding operational directives	CISA	Fully implemented	CISA established a memorandum of agreement with DOD to immediately share directives applying to the information networks under their respective jurisdictions.
Evaluate whether to adopt any guidance contained in an order or directive issued by DOD or DHS consistent with these procedures	CISA	Fully implemented	

Appendix III: Assessment of Leadership and Oversight Requirements in Executive Order 14028

Requirement in Executive Order 14028	Leadership and Oversight Agency	Implementation Status	Details on Implementation Status
Removing Barriers to Sharing Threat Information			
Notify the Assistant to the President for National Security Affairs and OMB of the evaluation described in this section within seven days of receiving notice of an order or directive issued consistent with the procedures in this section	CISA	Fully implemented	CISA and DOD included in their memorandum of agreement timing requirements for notifying and consulting with each other regarding planned directives. CISA also provided an example of its deliberations in deciding whether to take action related to a DOD directive, and of communicating this decision to the Assistant to the President for National Security Affairs.
Improving the Federal Government’s Investigative and Remediation Capabilities			
Provide OMB recommendations on requirements for logging events and retaining other relevant data within an agency’s systems and networks. These requirements should be designed to permit agencies to share log information to CISA and the Federal Bureau of Investigation.	CISA	Fully implemented	CISA provided OMB with recommendations to develop policies for logging, log retention, and log management. Among other things, CISA’s recommendations discussed required data that agencies should collect for each log event, and user behavior analytics that agencies should implement to identify potentially malicious activity.
Formulate policies for agencies to establish requirements for logging, log retention, and log management	OMB	Fully implemented	OMB issued guidance that established a maturity model to guide agency implementation requirements for event logging. The model established four tiers of maturity for event logging to help agencies understand how to achieve full compliance with logging requirements.
Work with agency heads to ensure that agencies have adequate resources to comply with requirements for logging, log retention, and log management	OMB	Partially implemented	OMB provided guidance to agencies to improve their log retention and log management practices and capabilities. However, OMB did not demonstrate that it had worked with agencies to ensure they had adequate resources to implement logging, log retention, or log management.

Source: GAO analysis of documentation from Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB). | GAO-24-106343

^aIn December 2021, a vulnerability was discovered in the Apache Log4j framework, which is a type of cyber security logging software used in websites and web applications across the world. The vulnerability, if left unmitigated, could allow malicious individuals to break into online-based systems, including cloud services and applications, to compromise data.

^bAccording to the Cyber Safety Review Board, the group known as Lapsus\$ exploited systemic ecosystem weaknesses to infiltrate and extort organizations for attention and public notoriety. For more details on this review, see *Cyber Safety Review Board, Review of the Attacks Associated with Lapsus\$ and Related Threat Groups* (Jul. 24, 2023).

^cThis Unified Coordination Group was created to coordinate the federal government’s response to the SolarWinds incident on December 16, 2020.

Appendix IV: Comments from the Department of Homeland Security

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



**Homeland
Security**

March 26, 2024

Marisol Cruz Cain
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-24-106343, "CYBERSECURITY:
Implementation of Executive Order Requirements Is Essential to Address Key
Actions"

Dear Ms. Cruz Cain,

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 recognition that the Cybersecurity and Infrastructure Security Agency (CISA) implemented—either partially or fully—31 of 32 leadership and oversight requirements for which CISA had responsibility in Executive Order (EO) 14028, "Executive Order on Improving the Nation's Cybersecurity," dated May 12, 2021.¹ As the nation's lead agency for protecting the federal civilian government and critical infrastructure against cybersecurity threats, CISA serves a central role in implementing this Executive Order, which makes a significant contribution toward increasing the security of the federal government's networks, including enabling greater visibility into cybersecurity threats, advancing incident response capabilities, and driving improvements in security practices for key information technology used by federal agencies. DHS remains committed to safeguarding federal computer systems by, among other actions, CISA reviewing major cyber incidents to reduce future risk and leveraging CISA's role in federal cybersecurity to drive dialogue on the security of the software used by federal agencies.

¹ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

**Appendix IV: Comments from the Department
of Homeland Security**

The draft report contained six recommendations, including three for DHS—two with which the Department concurs (Recommendations 1 and 3) and one with which the Department non-concurs (Recommendation 2), because leadership believes the intent of the recommendation has already been met. 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: 2024.03.26 06:57:11 -0400

JIM H. CRUMPACKER

Director

Departmental GAO-OIG Liaison Office

Enclosure

**Appendix IV: Comments from the Department
of Homeland Security**

**Enclosure: Management Response to Recommendations
Contained in GAO-24-106343**

GAO recommended that the Secretary of Homeland Security direct the Director of CISA to:

Recommendation 1: Issue, in a timely manner, its list of software and software product categories that are considered critical software.

Response: Concur. CISA's Cybersecurity Division (CSD) will identify and make available to federal agencies a list of example software products that fall within each of the 11 categories² of critical software, as defined by National Institute of Standards and Technology. Once complete, CSD will provide the list to Federal agencies for use, as appropriate. Estimated Completion Date (ECD): September 30, 2024.

Recommendation 2: Direct the Cyber Safety Review Board [CSRB] to conduct a review into the December 2020 SolarWinds cyber incident as required by Executive Order 14028.

Response: Non-concur. The CISA Director believes that the intent of this recommendation has already been met by the inclusion of information relating to the December 2020 SolarWinds cyber incident in the CSRB report, "Review of the December 2021 Log4j Event," dated July 11, 2022.³ Specifically, EO 14028 directed the development of a report on the SolarWinds hack within 90 days. However, given the amount of time required to establish the CSRB, solidify the member list, and begin research, the deadline was unachievable. Further, by the time the CSRB was operational and ready to conduct its inaugural review, a vulnerability, known as Log4j was identified.

Given that CISA had previously conducted independent research into the causes and impacts of the SolarWinds hack, with findings published in a webpage entitled, "Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise, dated May 14, 2021,"⁴ the CISA Director provided the CSRB with tasking guidance in February 2022 to incorporate information on the SolarWinds event into its review of Log4j. Accordingly, the CSRB followed the tasking guidance and the July 11, 2022, report includes numerous references and analysis of the SolarWinds event that fulfils the intent of the EO 14028 direction to conduct a review of this incident. Leadership believes that directing the CSRB to conduct another review of the SolarWinds

² <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory>

³ <https://www.cisa.gov/sites/default/files/2023-02/CSRB-Report-on-Log4j-PublicReport-July-11-2022-508-Compliant.pdf>

⁴ <https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directory-m365-compromise>

**Appendix IV: Comments from the Department
of Homeland Security**

event would be duplicative of prior work and an imprudent use of resources. We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 3: Direct the Cyber Safety Review Board [CSRB] to document steps taken or planned to implement the recommendations provided to the President for improving the board's operations.

Response: Concur. CISA's Stakeholder Engagement Division (SED) is responsible for supporting CSRB, and is therefore responsible for tracking the implementation of all CSRB recommendations provided to and approved by the President in the report entitled, "Review of the Inaugural Proceedings of the Cyber Safety Review Board," dated October 18, 2022.⁵ CISA SED has already taken steps consistent with these recommendations, such as establishing the Office of the National Cyber Director as a standing member of the CSRB. SED will continue work to implement recommendations from this report and will establish a process for documenting steps already taken or planned to address these recommendations. ECD: December 31, 2024.

⁵ https://www.cisa.gov/sites/default/files/2023-04/cyber_safety_review_board_review_of_inaugural_proceedings_508c.pdf

**Accessible Text follows for Appendix IV: Comments
from the Department of Homeland Security**

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation

Washington, DC 20201

December 15, 2023

Mary Denigan-Macauley
Director, Health Care
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Denigan-Macauley:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "PUBLIC HEALTH PREPAREDNESS: HHS Emergency Agency Needs to Strengthen Workforce Planning" (GAO-24-106108)

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

Sincerely,
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 – PUBLIC HEALTH PREPAREDNESS: HHS EMERGENCY AGENCY NEEDS TO STRENGTHEN WORKFORCE PLANNING (GAO-24-106108)

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity to review the Government Accountability Office (GAO) draft report assessing and reviewing workforce planning. HHS concurs with GAO's findings in this report related to ensuring there is a well-trained and resourced workforce to meet the Administration for Strategic Preparedness and Response's (ASPR) critical mission to lead the nation's response to public health and medical emergencies. However, one critical consideration is that when GAO began this review and audit, ASPR was in the initial planning stage of building its own internal human resources function as the Administration transitioned from a Staff Division within HHS to an Operating Division. As ASPR continues efforts to finalize and implement the Administration's internal human resources function, this report may not fully reflect the totality of activities and assessments have moved forward since GAO began the audit in 2022. HHS looks forward to providing additional information and data related to how the public health workforce will position to effectively prepare and respond to emerging health crisis in the future as functions and processes finalize.

Recommendation 1

The Assistant Secretary for Preparedness and Response should establish specific goals for its new in-house hiring office and related performance measures to help to ensure the agency improves hiring capabilities as intended. This could include goals and performance measures to help address areas of concerns the new office was intended to address, including time-to-hire, service quality, and unique workforce needs.

HHS Response

As previously shared with GAO and also described in the ASPR's key supporting documents, to include the Business Case, Addendum and Transition Plan, ASPR has identified goals and performance measures for its in-house hiring office. Specifically, the ASPR business case describe a specific cost-saving goal of an estimated \$7M, accomplished by bringing all hiring in-house and developing a 10-business-day workflow to issue tentative job offers to select candidates, which would result in an 80% decrease in the time to hire Critical Mission Occupations, Senior Executive Service (SES) and Title 42 positions. Further, the Addendum outlines specific hiring goals for each of the transition years along with planned activities to be transitioned. Lastly, the ASPR transition plan includes specific activities with measures and goals including the development of a Transition Project Management Office (PMO).

As previously shared with GAO, ASPR's OHC is establishing guidelines, timeframes, and process maps with Key Performance Indicators (KPIs) to be finalized by August 2024.

Recommendation 2

The Assistant Secretary for Preparedness and Response should develop tailored recruitment and hiring strategies to address government-wide shortages of human capital staff to meet the hiring needs of its in-house hiring office.

HHS Response

As previously shared with GAO, ASPR's OHC currently has 34 staff members and has identified an additional 41 positions tailored to enhance hiring capacity and capabilities of the Administration. This position target is based upon queries with other Operational Division Human Capital Directors that compared the size of their respective staffs. The ASPR OHC has also undergone an internal reorganization within its office and established a new organizational construct, which is designed to cover all components of the human capital cycle. The development of this new organization provided the analysis used by ASPR OHC to ensure that all anticipated human capital work would be covered within the new staffing model. ASPR also conducted an internal skills assessment for existing staff as part of this comprehensive approach.

In addition, ASPR has developed hiring plans to include the use of all available hiring flexibilities, consideration of recruitment and retention bonuses as applicable, and establishment of a liaison with the Department's OHR to determine interest in SROC staff moving to ASPR's OHC. All hiring actions are tracked through ASPR's transition PMO and a summary is provided to both ASPR and Departmental leadership on a monthly basis. ASPR continues to develop and implement recruitment and hiring strategies generally to support efforts to fill the identified vacancies in OHC as current efforts are assessed.

Recommendation 3

The Assistant Secretary for Preparedness and Response should identify critical areas that need workforce assessments and develop plans to implement such assessment, before its planned in-house hiring office is fully established. Such plans could include determining which assessments need to be conducted, when they will be conducted, and related resource needs.

HHS Response

HHS concurs with GAO's recommendation.

To date, ASPR's has identified critical skills and competencies to support our contracting, supply chain monitoring, and human capital programs by evaluating the

current and future portfolio of work. Most recently, ASPR's IBMSC Office identified critical skills and competencies to support the office by evaluating the current and future portfolio of work. ASPR shared this effort with GAO as apart of HHS October 2023 updated Statement of Actions for GAO-22-105397 and these efforts were reflected by GAO at that time.

ASPR will continue to support assessment efforts as planned in-house hiring commences, resource dependent, to address GAO's recommendation.

Recommendation 4

The Assistant Secretary for Preparedness and Response should conduct an agency-wide workforce assessment—that considers workforce needs identified by individual area assessments and available resources—to prioritize the skills and competencies of greatest need to achieve agency-side goals and mission, as identified in its strategic plan.

HHS Response

HHS concurs with GAO's recommendation.

As part of its existing strategic goal to ensure workforce readiness through development of innovative workplace practices, ASPR continues to focus on conducting an agency-wide workforce assessment to identify critical skills and competencies required to support and serve ASPR's mission. As described in response to Recommendation 3, ASPR has already identified critical skills and competencies in several programmatic areas of the agency, including contracting staff, human capital staff and supply chain monitoring. In addition, throughout 2023, ASPR's Office of Administration - which houses ASPR's information technology, financial, human capital, facilities, and contracting staff - conducted a pilot on workforce planning, which involved identifying skill gaps and training needs, as well as recruitment and retainment of employees with specialized competencies and/or knowledge. The pilot will inform future workforce assessments conducted across ASPR. ASPR will continue to support similar efforts, resource dependent, to address GAO's recommendation.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, (202) 512-5017 or cruzcainm@gao.gov.

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Rosanna Guerrero (Assistant Director), Shaun Byrnes (Analyst in Charge), Amanda Andrade, Ben Atwater, Tommy Baril Jr., Tracey Bass, Chris Businsky, Donna Epler, Franklin Jackson, Joe Kirschbaum, Evan Kreienseck, Michael Lebowitz, Steven Lozano, Scott Pettis, David Sadnavitch, Jonah Silencieux, Andrew Stavisky, and Adam Vodraska.

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