U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Report to Congressional Committees

Cybersecurity

Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans



November 18, 2026 | GAO-27-108661

Contents

Highlights ii

What GAO Found ii

What GAO Recommends ii

Why GAO Did This Study ii

Recommendations for Executive Action iv

Report 1

Introduction 1

Objectives 1

Background 1

Most, but Not All, Selected Agencies Addressed Guidance on Zero Trust Architecture Planning 6

Conclusions 14

Agency Comments and Our Evaluation 14

How GAO Did This Study 14

Extent to Which Selected Agencies Addressed Requirements and Guidance 19

Comments from Agencies 22

References 50

Accessible Data for Figures 54

About GAO 56

Cybersecurity

Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans

GAO-27-108661 November 18, 2026

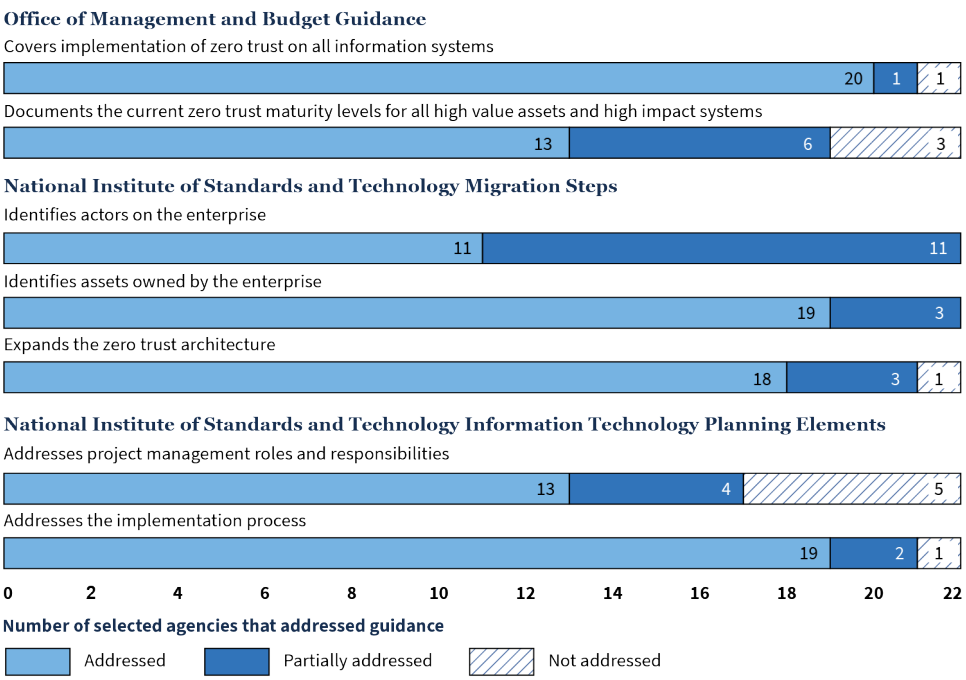
A report to congressional committees

For more information, contact Jennifer R. Franks at FranksJ@gao.gov or David B. Hinchman at HinchmanD@gao.gov.

What GAO Found

A zero trust architecture (ZTA) is a set of cybersecurity principles that state that organizations must verify everything that attempts to access their systems and services. Almost all of the 22 agencies in this review had plans for zero trust architectures in their information technology (IT) environments. ZTA implementation will evolve over time as technology changes. As of August 2026, five agencies had addressed guidance from the Office of Management and Budget (OMB) or National Institute of Standards and Technology (NIST) in their ZTA planning. However, 17 agencies had not fully done so.

Extent to Which 22 Civilian Chief Financial Officers Act of 1990 Agencies Addressed Selected Federal Guidance in Their Zero Trust Implementation Plans



Source: GAO analysis of agencies' zero trust architecture implementation plans. | GAO-27-108661

Agency officials provided numerous reasons, including limited staffing and funding, for not fully addressing federal guidance. Nevertheless, agencies continue to implement zero trust on their systems. However, until these agencies address selected ZTA guidance in their zero trust implementation plans, they may risk not having what they need to fully establish and maintain zero trust architectures. For instance, agency management may not be able to adequately apply resources where they are needed to continue zero trust implementation. As a result, agencies may risk not being able to effectively employ a more modern, robust way of securing their assets. Agencies would therefore be at increased risk of cyberattacks that could interrupt operations or otherwise compromise agency resources.

What GAO Recommends

GAO is making a total of 40 recommendations to 17 agencies to address selected guidance. Thirteen agencies agreed with the recommendations, and several described planned actions to implement them. Four agencies neither agreed nor disagreed with the recommendations.

Why GAO Did This Study

To protect federal information and systems, the Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to protect the information and systems that support the agencies' operations and assets. One approach is to implement ZTA principles founded on the concept that no actor, system, network, or service operating outside of, or within, an organization's security perimeter should be trusted.

FISMA also includes a provision for GAO to periodically report to Congress on agencies' implementation of the act. This report examines the extent to which agencies' plans to implement zero trust architecture addressed selected federal guidance.

GAO assessed plans to implement zero trust architecture from 22 civilian Chief Financial Officer Act of 1990 agencies and assessed the agencies' compliance with selected OMB and NIST guidance, relevant to ZTA implementation and IT project planning. GAO also interviewed cognizant agency officials to better understand their zero trust planning efforts and to better understand the guidance they developed.

Recommendations for Executive Action

We are making a total of 40 recommendations to 17 of the 22 selected civilian Chief Financial Officers Act agencies. Specifically:

We are making the following two recommendations to the Department of Agriculture:

The Secretary of Agriculture should ensure that the department's Chief Information Officer documents the maturity levels of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 1)

The Secretary of Agriculture should ensure that the department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of fully identifying actors within its IT environment. (Recommendation 2)

We are making the following four recommendations to the Department of Commerce:

The Secretary of Commerce should ensure that the department's Chief Information Officer documents the maturity levels of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 3)

The Secretary of Commerce should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture. (Recommendation 4)

The Secretary of Commerce should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 5)

The Secretary of Commerce should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document the implementation process. (Recommendation 6)

We are making the following recommendation to the Department of Education:

The Secretary of Education should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the

National Institute of Standards and Technology zero trust migration step of fully identifying actors within its IT environment. (Recommendation 7)

We are making the following recommendation to the Department of Energy:

The Secretary of Energy should ensure that the department's Chief Information Officer updates its zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice of identifying actors within its IT environment. (Recommendation 8)

We are making the following six recommendations to the Department of Health and Human Services:

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully documents an enterprise-wide implementation plan for zero trust architecture that incorporates guidance from the Office of Management and Budget. (Recommendation 9)

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment as it documents its enterprise-wide plan. (Recommendation 10)

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of identifying assets within its IT environment as it documents its enterprise-wide plan. (Recommendation 11)

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture in documenting the department's enterprise-wide plan. (Recommendation 12)

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts in documenting the department's enterprise-wide plan. (Recommendation 13)

The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology practice to document the implementation process as it documents its enterprise-wide plan. (Recommendation 14)

We are making the following recommendation to the Department of Homeland Security:

The Secretary of Homeland Security should ensure that the department's Chief Information Officer fully documents the maturity levels for all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 15)

We are making the following three recommendations to the Department of Housing and Urban Development:

The Secretary of Housing and Urban Development should ensure that the Department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology migration step of identifying actors within its IT environment. (Recommendation 16)

The Secretary of Housing and Urban Development should ensure that the Department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology migration step of identifying assets within its IT environment. (Recommendation 17)

The Secretary of Housing and Urban Development should ensure that the Department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology practice to document the implementation process for its zero trust architecture. (Recommendation 18)

We are making the following four recommendations to the Department of the Interior:

The Secretary of the Interior should ensure that the department's Chief Information Officer documents the maturity levels for all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 19)

The Secretary of the Interior should ensure that the department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment. (Recommendation 20)

The Secretary of the Interior should ensure that the department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture. (Recommendation 21)

The Secretary of Interior should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 22)

We are making the following recommendation to the Department of Justice:

The Attorney General should ensure that the department's Chief Information Officer documents the maturity levels for all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 23)

We are making the following three recommendations to the Department of State:

The Secretary of State should ensure that the department's Chief Information Officer documents the maturity levels for all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 24)

The Secretary of State should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment. (Recommendation 25)

The Secretary of State should ensure that the department's Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 26)

We are making the following three recommendations to the Department of the Treasury:

The Secretary of the Treasury should ensure that the department's Chief Information Officer fully documents the maturity levels of all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 27)

The Secretary of the Treasury should ensure that the department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of fully identifying actors within its IT environment. (Recommendation 28)

The Secretary of the Treasury should ensure that the department's Chief Information Officer updates the department's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust architecture. (Recommendation 29)

We are making the following two recommendations to the Environmental Protection Agency:

The Administrator of the Environmental Protection Agency should ensure that the agency's Chief Information Officer updates the agency's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of fully identifying actors within its IT environment. (Recommendation 30)

The Administrator of the Environmental Protection Agency should ensure that the agency's Chief Information Officer updates the agency's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology practice of documenting project management roles and responsibilities for its zero trust efforts. (Recommendation 31)

We are making the following recommendation to the National Aeronautics and Space Administration:

The Administrator of the National Aeronautics and Space Administration should ensure that the administration's Chief Information Officer fully documents the maturity levels of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 32)

We are making the following two recommendations to the Nuclear Regulatory Commission:

The Chairman of the Nuclear Regulatory Commission should ensure that the commission's Chief Information Officer updates the commission's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment. (Recommendation 33)

The Chairman of the Nuclear Regulatory Commission should ensure that the commission's Chief Information Officer updates the commission's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 34)

We are making the following recommendation to the National Science Foundation:

The Director of the National Science Foundation should ensure that the foundation's Chief Information Officer updates the foundation's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 35)

We are making the following four recommendations to the Office of Personnel Management:

The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment. (Recommendation 36)

The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying assets within its IT environment. (Recommendation 37)

The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust architecture to fully

address the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture. (Recommendation 38)

The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts. (Recommendation 39)

We are making the following recommendation to the Small Business Administration:

The Director of the Small Business Administration should ensure that the administration's Chief Information Officer documents the maturity levels of all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency. (Recommendation 40)

Introduction

Federal agencies rely heavily on information technology (IT) systems to carry out their missions, making the security of these systems vital due to the sensitive and essential data they contain. Moreover, these systems face increasing risks, not only from insider threats, but also from the external threats of malicious attackers. As such, maintaining rigorous cybersecurity programs that provide timely, relevant, and accurate information is imperative.

A modern, robust approach to securing information and systems includes the implementation of zero trust architecture (ZTA) principles. Such principles are founded on the concept that no actor, system, network, or service operating outside of, or within, an organization's security perimeter should be trusted. Instead, the principles suggest that organizations must verify anything and everything that attempts to establish access to their systems, services, and networks. According to the Cybersecurity and Infrastructure Security Agency (CISA), as the technology landscape continues to evolve, new solutions and continued discussions on how to best achieve zero trust objectives are paramount.[1] Therefore, zero trust architecture implementation will continue to evolve over time.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement information security programs to protect the information and systems that support the agencies' operations and assets.[2] FISMA also includes a provision for GAO to periodically report to Congress on agencies' implementation of the act.

Objectives

Our specific objective for this review was to determine the extent to which agencies' plans to implement zero trust architecture addressed selected federal guidance. For this review, we assessed 22 of the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies.[3] A full description of our scope and methodology can be found at the end of this report.

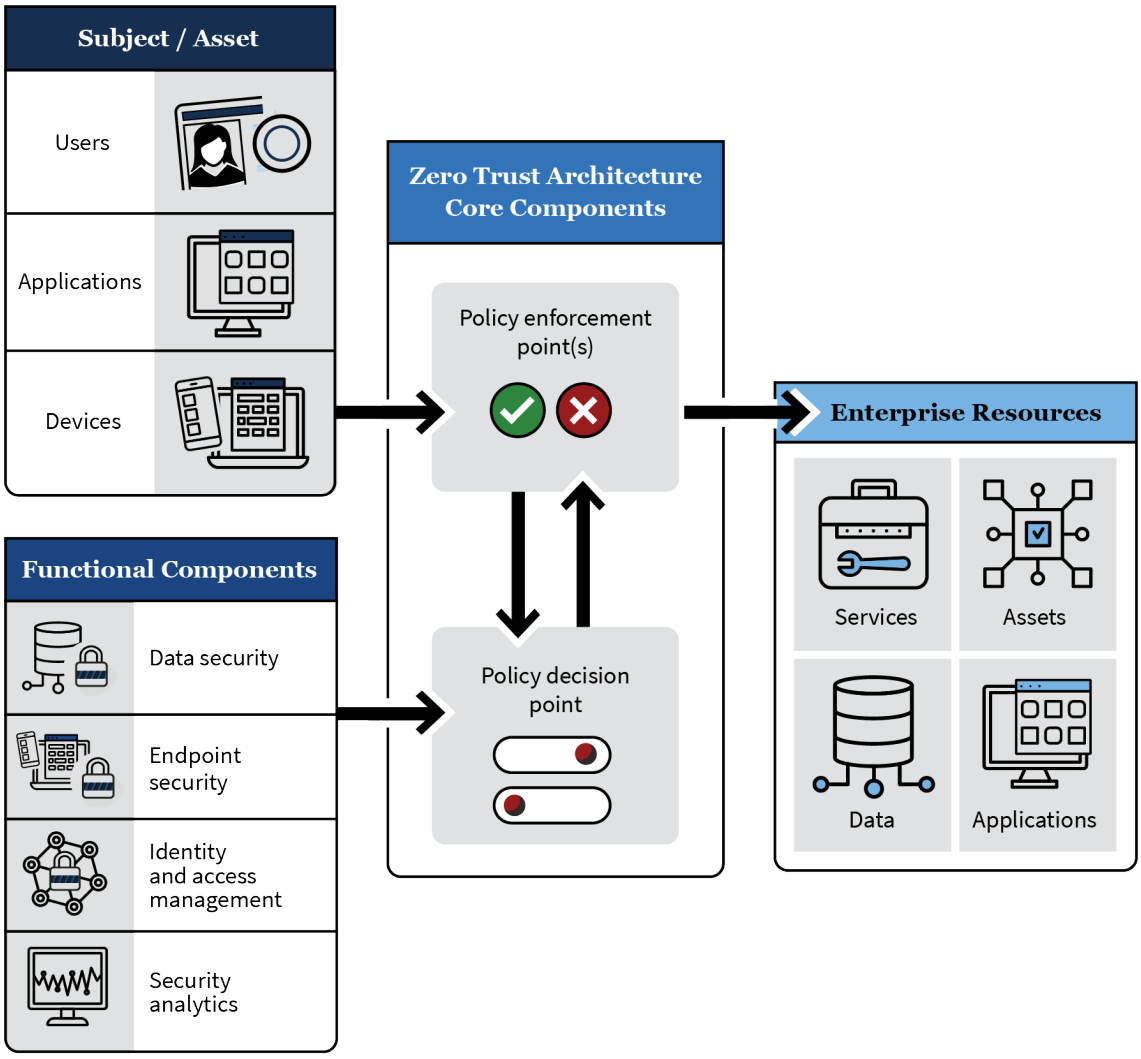
Background

According to National Institute of Standards and Technology (NIST) guidance, zero trust architecture is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy. ZTA is based on an acknowledgment that threats exist both inside and outside traditional network boundaries.

NIST states that at a high level, zero trust architectures grant resource access to a given subject using policy decisions. The architectures use policy enforcement points that enable, monitor, and eventually terminate connections between a subject and enterprise resources.[4] For example, if a user wants to access a resource (e.g. a database), the user must be approved by

the policy decision point and granted access by the policy enforcement point. The policy decision point uses inputs from the functional components in its decision-making procedures. Figure 1 shows a notional organization of the zero trust components, including the policy decision and policy enforcement points, elements used in access decisions, and the purposes the components serve in providing or denying user access to enterprise resources.

Figure 1: High-Level Zero Trust Architecture Concept



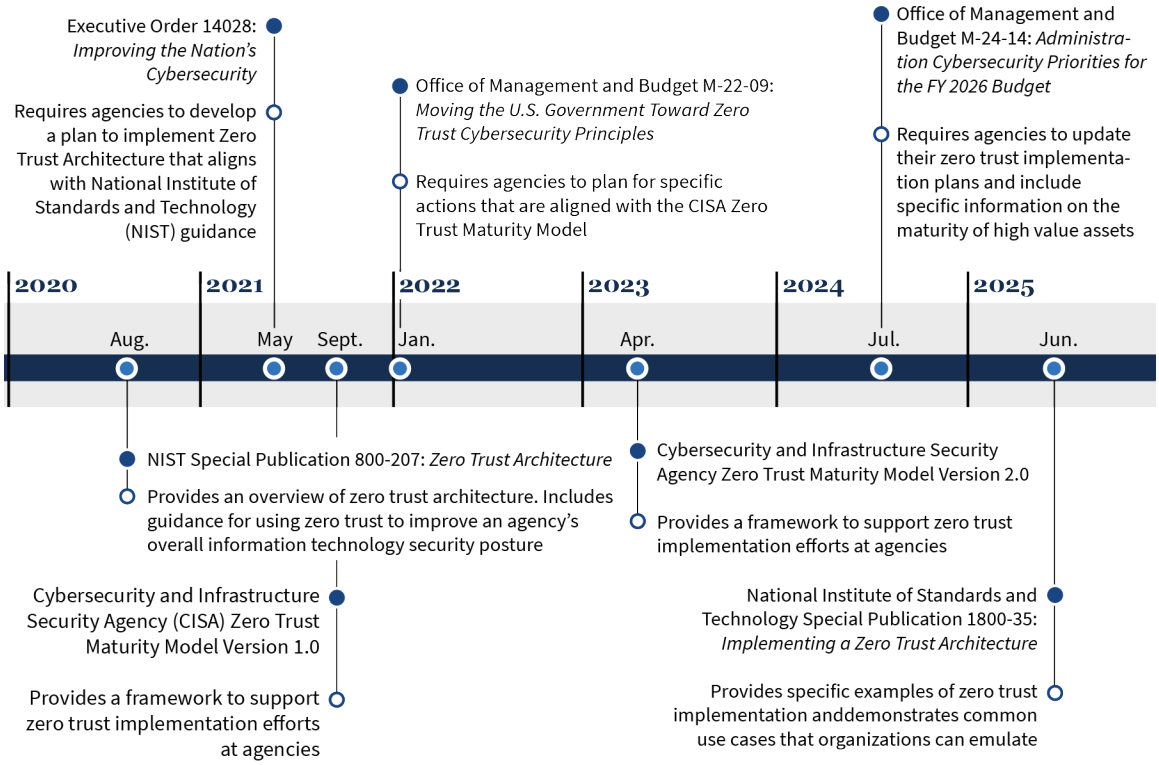
Sources: GAO interpretation of National Institute of Standards and Technology zero trust architecture concept; lembergvector/stock.adobe.com (icons). | GAO-27-108661

Federal Guidance on Zero Trust Architecture Has Evolved

Federal agencies with responsibilities related to government-wide efforts to implement zero trust architecture have developed relevant guidance for other federal agencies as they

transition towards ZTA. This guidance has evolved over time. Figure 2 shows a timeline of various sets of requirements and guidance across the government for ZTA.

Figure 2: Federal Guidance Concerning Zero Trust Architecture Over Time



Source: GAO analysis. | GAO-27-108661

NIST Guidance

As shown in the timeline, NIST first issued guidance on zero trust in 2020.[5] This publication provided information to agencies meant to aid in understanding ZTA for civilian unclassified systems, and to provide a road map to migrate and deploy relevant security concepts to an enterprise environment. Later, in 2025, NIST prepared additional guidance to provide agencies with examples of ZTA implementations and common use cases, including best practices and lessons learned.[6]

NIST has also published guidance to help agencies in managing large IT security projects, such as implementing zero trust architectures.[7] Its guidance can be used by both federal and private sector entities to enhance project management and implementation.

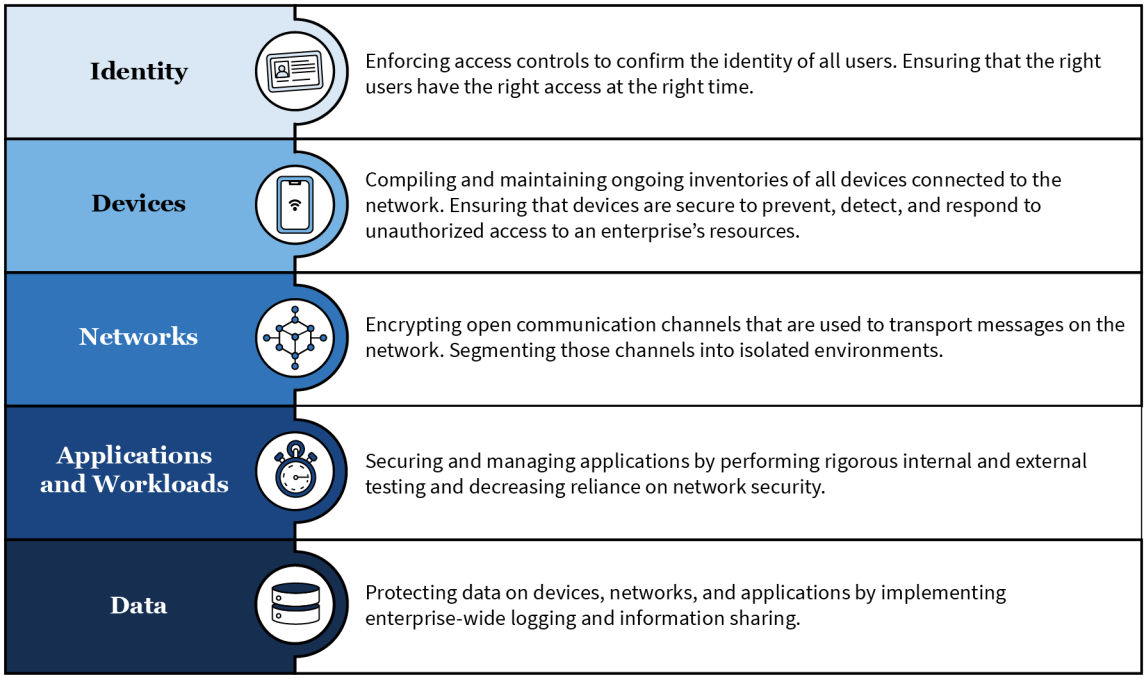
Executive Order

Executive Order 14028, issued in May 2021, stated that the federal government must improve its efforts to identify, deter, protect against, detect, and respond to cyber threats to the public and private sectors and the American people's security and privacy.[8] The order outlined actions that the federal government must take in five areas. One of these areas corresponds to the federal government's efforts to implement ZTA.

CISA Guidance

In response to Executive Order 14028, CISA released its *Zero Trust Maturity Model*, which is intended to aid agencies in implementing ZTA.[9] The model is intended to support agencies in a rapidly evolving environment and technology landscape by focusing on modernization efforts related to zero trust. CISA organized its maturity model across five pillars that support the foundation of zero trust: identity, devices, networks, applications and workloads, and data. Figure 3 describes these five pillars.

Figure 3: The Cybersecurity and Infrastructure Security Agency's Five Pillars of Zero Trust Architecture



Sources: GAO analysis of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model Version 2.0 and other relevant federal policies and guidance; narathip/stock.adobe.com (icons). | GAO-27-108661

Further, each of the pillars is assigned four rating levels intended to define the maturity of an organization's transition to ZTA—traditional, initial, advanced, and optimal.[10] The maturity ratings are intended to provide agencies an understanding of the zero trust capabilities that

are associated at each of these levels, iteratively building towards more effective protections at each level. CISA describes how aspects of each pillar change with increasing maturity. Cross-pillar coordination helps advance zero trust capabilities throughout all pillars. Each pillar needs ongoing improvement, and their progress depends on the development of capabilities in the other pillars.

OMB Guidance

In January 2022, the Office of Management and Budget (OMB) published a strategy that requires agencies to meet specific cybersecurity standards and objectives intended to reinforce the government's defenses against sophisticated and persistent threat campaigns.[11] The strategy outlines actions that agencies were to take by the end of fiscal year (FY) 2024 that are intended to form a starting point to implementing zero trust architecture.[12] The actions are organized using the Zero Trust Maturity Model by CISA.

In July 2024, OMB published guidance concerning agencies' FY 2026 budget priorities, which included expectations concerning zero trust architecture.[13] Specifically, the guidance states that agencies are to incorporate all of their IT systems into their zero trust planning, among other requirements, but did not establish a deadline for implementing zero trust on all information systems.

Guidance from OMB and NIST Can Improve Agency Zero Trust Implementation

As mentioned above, OMB and NIST have both established guidance to aid agencies in their implementation of zero trust. If implemented effectively, various elements from this guidance could improve agencies' zero trust implementation planning processes. Table 1 presents elements from OMB and NIST guidance that could enhance agency zero trust implementation plans if included.

Table 1: Guidance Elements from the Office of Management and Budget and National Institute of Standards and Technology for Agency Zero Trust Planning

Guidance document	Element to address in zero trust plan
Office of Management and Budget Memorandum M-24-14[a]	Covers implementation of zero trust on all information systems
	Documents the current zero trust maturity levels for all high value assets and high impact systems
National Institute of Standards and Technology Special Publication 800-207 Migration Steps[b]	Identifies actors on the enterprise
	Identifies assets owned by the enterprise
	Expands the zero trust architecture
National Institute of Standards and Technology Special Publication 800-35 IT Planning Elements[c]	Addresses project management roles and responsibilities
	Addresses the implementation process

Source: GAO selection of federal guidance relevant to zero trust architecture. | GAO-27-108661

[a]Office of Management and Budget, Administration Cybersecurity Priorities for the FY 26 Budget, M-24-14 (Washington, D.C.: Jul. 10, 2024). Requires agencies to incorporate into their zero trust planning elements of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model, version 2.0 (Arlington, VA: April 2023).

[b]National Institute of Standards and Technology, Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: August 2020).

[c]National Institute of Standards and Technology, Guide to Information Technology Security Services, Special Publication 800-35 (Gaithersburg, MD: October 2003).

Recent GAO Work on Zero Trust

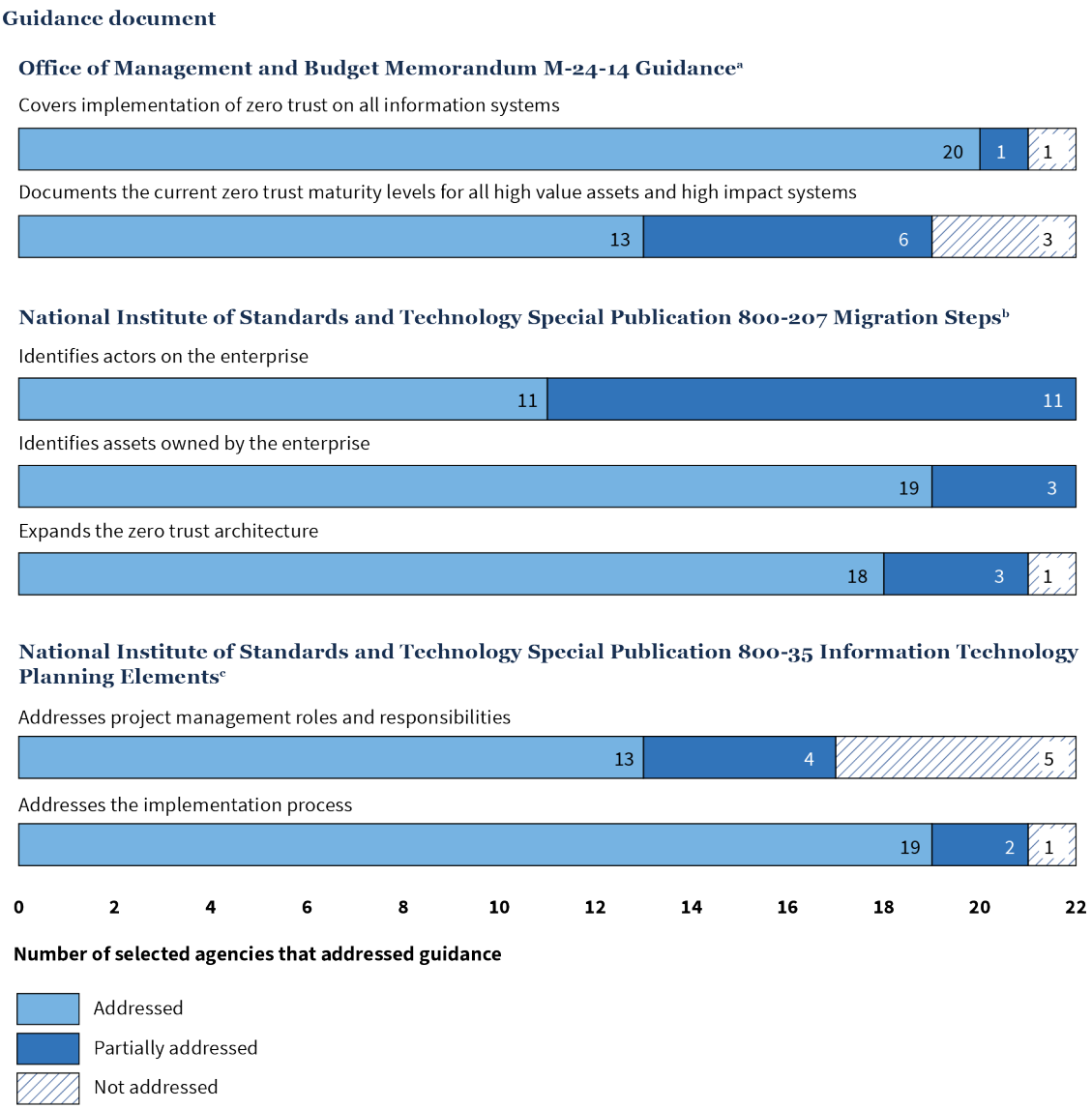
In November 2022, we issued a Science & Technology Spotlight on zero trust architecture.[14] This product provided an overview of what zero trust architecture is, some of the opportunities associated with zero trust implementation, as well as some policy context and questions associated with zero trust architecture.

Also in November 2022, we reported on progress that the United States Secret Service had made in developing an implementation plan to support zero trust architecture.[15] In that report, we made two recommendations to the Secret Service to improve its planning. Secret Service has implemented one of our recommendations. As of August 2026, one additional recommendation remained open.

Most, but Not All, Selected Agencies Addressed Guidance on Zero Trust Architecture Planning

As of August 2026, over half of selected agencies had addressed OMB and NIST guidance regarding zero trust plans, migration steps, and IT planning. However, multiple agencies partially addressed or did not address all of the guidance. Figure 4 presents the extent to which the 22 agencies addressed OMB and NIST guidance in their zero trust plans. A more detailed discussion of these findings follows the graphic. Appendix I provides a full list of the extent to which selected agencies had addressed relevant guidance.

Figure 4: Extent to Which 22 Civilian Chief Financial Officers Act Agencies Addressed Selected Federal Guidance in Their Zero Trust Implementation Plans as of August 2026



Source: GAO analysis of agencies' zero trust architecture implementation plans. | GAO-27-108661

[a]Office of Management and Budget, Administration Cybersecurity Priorities for the FY 26 Budget, M-24-14 (Washington, D.C.: Jul. 10, 2024). Requires agencies to incorporate into their zero trust planning elements of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model, version 2.0 (Arlington, VA: April 2023).
[b]National Institute of Standards and Technology, Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: August 2020).
[c]National Institute of Standards and Technology, Guide to Information Technology Security Services, Special Publication 800-35 (Gaithersburg, MD: October 2003).

Most Agencies Addressed Selected OMB Guidance in Their Zero Trust Plans

Zero Trust Implementation Plan Coverage of Information Systems

OMB's 2024 guidance required agencies to develop plans that cover the implementation of zero trust on all of their information systems.[16] Twenty of the 22 agencies—the Departments of Agriculture (USDA), Commerce, Education, Energy, Homeland Security (DHS), Housing and Urban Development (HUD), the Interior, Justice (DOJ), Labor, State, Transportation (DOT), the Treasury, Veterans Affairs (VA), the Environmental Protection Agency (EPA), General Services Administration (GSA), Nuclear Regulatory Commission (NRC), National Science Foundation (NSF), Office of Personnel Management (OPM), Small Business Administration (SBA), and Social Security Administration (SSA)—developed plans to implement zero trust architecture that covered all of their information systems. However, one agency developed a plan that only partially covered its systems, and one agency had not developed a plan that covered all of its systems. Specifically:

- The National Aeronautics and Space Administration (NASA) developed a plan that addressed one of its three enterprise environments but did not address the other two. In 2025, NASA's Inspector General made a recommendation to address this shortcoming.[17]
- In addition, the Department of Health and Human Services (HHS) did not develop an enterprise-wide plan for ZTA implementation that included all of its information systems. Instead, HHS was tracking the maturity of ZTA implementation at its operating divisions based on CISA's maturity model.[18] Officials from HHS stated that in their large, federated agency, officials are tracking zero trust implementation across a multitude of component agencies instead of developing a centralized plan.

Until HHS develops plans to implement ZTA that cover the implementation of zero trust on all of their information systems, its management will likely not have a coherent view of disparate activities associated with the transition to zero trust. As such, HHS will be at risk that some of its systems may not reap the benefits of a modern, robust approach to cybersecurity, putting its systems and data at risk.

Documentation of System Maturity Levels

OMB's guidance also required that agencies document the current zero trust maturity for their high-value assets (HVA) and high-impact systems[19] based on the levels developed by CISA across each of the zero trust pillars.[20]

Thirteen of the 22 agencies—Education, Energy, HHS, HUD, Labor, DOT, VA, EPA, GSA, NRC, NSF, OPM, and SSA—documented current maturity levels for all of their HVAs and high-impact systems. In addition, six agencies partially documented maturity levels, while the three remaining agencies did not document maturity levels for any of their HVAs or high-impact systems. Specifically:

- DHS, Interior, DOJ, State, the Treasury, and NASA were each tracking the maturity of HVAs and high-impact systems. However, none of these six agencies had fully documented the maturity of all of their HVAs or high-impact systems in doing so.

  Officials from DHS stated that lengthy periods of government shutdown over the past fiscal year limited the department's ability to assess and document the maturity metrics for HVAs or high-impact systems' implementation. Interior officials stated that they did not assess or document all of their HVAs because not all of their HVAs are network-connected due to their sensitive nature. They added that those HVAs are related to operational technology and are isolated to prevent compromise. Nevertheless, according to CISA, isolating systems from the network is not sufficient to guarantee security.[21] DOJ officials stated that due to resource constraints, the agency was unable to fully assess and document maturity. Officials from State did not provide a reason for partially documenting maturity levels. Treasury officials stated that the department has an automated system that allows system owners to input the maturity of their systems. They added that any missing systems would be due to owners not having updated the information, or a problem with the automated system. NASA officials stated that the way they scored their information environment was different than the approach that OMB required for HVAs and high-impact systems, and therefore, NASA was unable to get responses from all of the system owners.

- USDA, Commerce, and SBA had not documented the zero trust maturity levels of their HVAs or high-impact systems. USDA officials stated that the department is reviewing its zero trust plan and strategy with plans to incorporate maturity levels for its HVAs and high-impact systems because the requirement was established after USDA published its documents. Officials from Commerce stated that staffing losses significantly constrained the ability to sustain the department's zero trust working group. They also stated that these resource limitations impeded efforts to produce comprehensive documentation, including documentation of zero trust maturity for high value assets. SBA officials did not provide a reason for not documenting maturity levels.

Until agencies fully document the maturity of ZTA on all of their HVAs and high-impact systems, agency leadership will not have the visibility they need into agency zero trust posture. As such, they may not be able to adequately plan for the additional resources required to continue implementing zero trust architectures.

Not All Agencies Fully Addressed Selected NIST Zero Trust Migration Steps

NIST's 2020 guidance established migration steps that agencies can leverage to ensure awareness of the foundational state of their IT environments before ZTA deployment is possible.

Identification of Actors on the Enterprise

According to NIST, for a zero trust enterprise to operate, the policy engine must have knowledge of enterprise subjects (i.e. actors),[22] which could include human and non-person entities.[23] Eleven of the 22 agencies—Commerce, DHS, Labor, DOJ, DOT, GSA, VA, NASA, NSF, SBA, and SSA—documented procedures intended to identify actors within their zero trust IT environment. However, 11 agencies partially documented procedures. Specifically:

USDA, Education, Energy, HHS, HUD, Interior, State, Treasury, EPA, NRC, and OPM partially included steps to identify actors on their enterprises within their zero trust plans.[24] For instance, the agencies had documented procedures to identify users within their IT environments such as through the use of the Continuous Diagnostics and Mitigation program.[25] However, these agencies had not documented procedures for identifying non-person entities within those environments.

USDA officials stated that the exclusion of non-person entities was an oversight, and that the department is reviewing its documentation with plans to identify all actors. Education officials stated that the department's initial ZTA investments prioritized human-centric identity risks because these areas represented the highest-impact, highest-probability threat vectors, and could be directly mitigated with the limited ZTA modernization funding available at the time. Energy officials stated that they have a project underway that will result in the inclusion of non-person entities within their records.

In addition, HUD officials stated that the department is working to integrate identity with applications, but that the effort was a work in progress. Treasury officials stated that when the department initially developed its ZTA plan, it did not have non-person entities operating within its environment. They stated that the department plans to incorporate these in future plans. OPM officials stated that the agency can identify users and most devices on its network, but this is not documented in its ZTA plan. Interior officials stated that the staff who created the ZTA plans were no longer with the department. They added that the department will include identity management for non-person entities in future zero trust planning activities.

NRC officials stated that when the department developed and updated its ZTA plan for OMB, they focused on OMB guidance and not NIST guidance; therefore, the inclusion of non-person entities was implicit but not specifically documented in its plan. HHS, State, and EPA did not provide reasons for the lack of inclusion of non-person entities.

Until agencies fully document their approaches to meeting NIST's guidance concerning the identification of actors within their zero trust environments, they run the risk that they will not have a process in place to achieve full visibility into the human and non-person entities that are accessing their resources. As such, agencies may not be able to adequately ensure that the right users are accessing the right resources at the right time.

Identification of Assets Owned by the Enterprise

NIST further suggests that one of the key requirements of ZTA is the ability to identify and manage devices. NIST guidance states that this ability goes beyond simply cataloging and maintaining a database of assets to include configuration management and monitoring. Of the 22 agencies, 19—USDA, Commerce, Education, Energy, DHS, Interior, DOJ, Labor, State, DOT, Treasury, VA, EPA, GSA, NASA, NRC, NSF, SBA, and SSA—outlined procedures to identify assets owned by their enterprises. Three selected agencies had partially done so. Specifically:

HHS, HUD and OPM had partially described efforts to identify assets. The agencies described plans to identify assets but not to manage the configuration of those assets owned by their enterprises.

HHS officials stated that the department had a centralized asset inventory but did not provide a reason why the department had not addressed this fully in its zero trust documentation. HUD officials did not provide a reason why they had not addressed this fully in their zero trust documentation. In addition, OPM officials stated that they have a tool to perform hardware asset management, but that the tool is not a unified management platform.

Until agencies fully document their approaches to meeting NIST's guidance concerning the identification of assets within their zero trust environments, they run the risk that they will not have a process in place to achieve full visibility into the devices operating on their environments. As such, agencies may not be able to prevent unauthorized access to their resources.

Expansion of Zero Trust Architecture

According to NIST guidance, once an enterprise enters the steady operational phase of ZTA, enterprise administrators can begin planning the next phase of zero trust deployment. Eighteen of the 22 agencies—USDA, Education, Energy, DHS, HUD, DOJ, Labor, State, DOT, Treasury, VA, EPA, GSA, NASA, NRC, NSF, SBA and SSA—fully described the expansion of their zero trust architectures in their planning documentation. However, three agencies partially did so, and one did not. Specifically:

- Commerce, Interior, and OPM partially described the expansion of their zero trust architecture. For example, the agencies had accounted for ZTA steps required by previous OMB guidance but had not outlined implementation efforts beyond those steps.[26] Commerce officials stated that staffing losses significantly constrained the ability to sustain the department's zero trust working group, which is responsible for coordinating and monitoring the department's ZTA activities. They said that these resource limitations also impeded efforts to produce comprehensive documentation. Interior officials did not provide a reason for not documenting the expansion of their zero trust. In addition, OPM staff stated that the department continues to expand its zero trust architecture, but they did not provide additional documentation of this.

- HHS officials stated that individual operating divisions were working to implement zero trust and added that the operating divisions have autonomy to plan and execute zero trust as they see fit. However, HHS has not documented how it intended to expand its ZTA department wide.

Until agencies fully document their approaches to meeting NIST's guidance concerning the expansion of their zero trust approach, they risk overlooking processes and procedures that will be required to implement ZTA within their IT environments. As such management may not have a coherent view of all of the disparate elements required for the transition to ZTA.

Not All Agencies Fully Addressed Selected NIST IT Planning Elements

In 2003, NIST developed guidance for organizations to consider when selecting, implementing, and managing IT security services. Such services could include ZTA. Particularly, the guidance states that an implementation plan provides a roadmap for an organization on moving from its current environment to a desired future environment. Zero trust plans for the 22 agencies in our review varied in the extent to which they addressed this NIST guidance.

Project Management Roles and Responsibilities

According to NIST guidance, an IT security implementation plan should identify the roles and responsibilities of individuals responsible for project management for both the implementation and operations phases. Thirteen of the 22 agencies—USDA, Education, Energy, DHS, HUD, DOJ, Labor, DOT, VA, GSA, NASA, SBA, and SSA—fully incorporated project management roles and responsibilities into their zero trust planning. However, four of the agencies had only partially done so, and five had not. Specifically:

- State, EPA, NSF, and OPM partially documented roles and responsibilities for their zero trust plans. For instance, State documented organizations that would be expected to have roles and responsibilities for ZTA but did not document the details of those responsibilities. EPA and OPM documented, at a high level, zero trust governance teams but did not identify the specific roles and responsibilities of individuals for zero trust implementation. NSF documented a list of roles and offices across the department with responsibility within cybersecurity operations. However, the plan did not specify how those roles and offices factor specifically into zero trust efforts.

  State, EPA, and OPM did not provide reasons for partially documenting roles and responsibilities. NSF officials stated that they did not include roles and responsibilities in their ZTA planning documentation because they focused on OMB guidance and not NIST guidance.

- Commerce, HHS, Interior, Treasury, and NRC did not identify zero trust implementation roles and responsibilities within their ZTA planning documentation.

Commerce officials stated that they had established a zero trust working group, which was subsequently paused due to staffing constraints. They said that they had documented roles and responsibilities for participation in the working group and for activities to be carried out. The officials added that the department intends to reestablish the working group and ensure these roles and responsibilities are reassessed and formally updated. HHS officials stated that operating divisions have autonomy to plan and execute zero trust as they see fit. However, HHS had not defined roles and responsibilities for ZTA at the department level.

Interior officials stated that funding and attrition issues resulted in Interior not having a dedicated zero trust organization. They added that new efforts to manage the planning, implementation, and reporting of zero trust within the department will be incorporated into the responsibilities of existing employees. In addition, Treasury officials stated that the department does not have a centralized project management structure, and that individual components, systems, and applications are responsible for ZTA efforts. However, Treasury's implementation plan did not define roles and responsibilities at the component level. NRC did not explain why they had not addressed this element in their zero trust planning documentation.

Until agencies document project management roles and responsibilities as suggested by NIST, management risks being unable to effectively target resources at the work needed to implement ZTA. As such, the agencies run the risk that they will not have staff in the right places to ensure that they can manage the path from the current state of their IT environments to the future state of incorporating zero trust within their IT environments.

Establishment of an Implementation Process

According to NIST guidance, program managers need to articulate their vision for implementing the IT security service. Nineteen of the 22 selected agencies—USDA, Education, Energy, DHS, Interior, DOJ, Labor, State, DOT, Treasury, VA, EPA, GSA, NASA, NRC, OPM, NSF, SBA and SSA—fully described their implementation process for ZTA. Two agencies partially described the process, and one had not done so. Specifically:

- Commerce and HUD partially documented their implementation process. For instance, Commerce provided responses to OMB concerning its zero trust efforts but had not updated its underlying ZTA plan since 2022. HUD provided detailed plans for implementing the Identity pillar but only discussed the M-22-09 requirements for the other pillars.[27]

  Commerce officials stated that staffing losses significantly constrained the ability to sustain the department's zero trust working group; these resource limitations also impeded efforts to produce comprehensive documentation on the department's ZTA implementation plan. HUD officials stated that their zero trust process began with the Identity pillar, and that they are beginning to invest in the other pillars; they explained that HUD has work to do to expand its ZTA planning.

Given that it had not developed an enterprise-wide plan to implement ZTA, HHS did not document its ZTA implementation process for the enterprise. HHS officials stated that operating divisions have autonomy to plan and execute zero trust as they see fit.

Until agencies fully implement IT planning steps as suggested by NIST, they run the risk that they will not accurately map out the path from the current state of their IT environments to the future state of incorporating zero trust within their IT environments. If they do not have a path mapped out, management may be unable to effectively target resources at the work needed to implement ZTA.

Conclusions

Federal IT systems face increasing risks, both from insider threats and external malicious actors, and protecting the information and systems that support agency operations and assets is imperative. Zero trust architecture is a modern, robust approach to securing an agency's technology enterprise and represents a paradigm shift in how federal organizations can think about protecting their IT assets.

To their credit, most of the 22 agencies we reviewed have plans to implement enterprise-wide zero trust architectures within their IT environments. However, only five of the 22 agencies (Labor, DOT, VA, GSA, and SSA) have fully addressed the OMB and NIST guidance on implementing zero trust architecture and IT planning discussed in this report. Many of the 22 agencies have done so only partially.

Absent a full implementation of ZTA requirements and guidance, agencies will lack an appropriate roadmap to fully incorporate and maintain an effective zero trust architecture. Until agencies have such a roadmap for this complex and ongoing effort, they will be challenged to fully reap the benefits of a modern, robust security approach that has been demonstrated to provide more effective asset protection across the technology enterprise. In the face of the abovementioned rising threats, it will be vital for agencies to fully implement federal requirements and better secure the government's technology assets. We are making a total of 40 recommendations to 17 of the 22 selected civilian Chief Financial Officers Act agencies, as listed in our Recommendations section.

Agency Comments and Our Evaluation

We provided a draft of this report to the 22 selected civilian CFO Act agencies and OMB for their review and comments. Of the 17 agencies to which we made recommendations, 13 agreed, and four did not agree or disagree. Of the six agencies to which we did not make recommendations, five agencies responded that they had no comments on the report, and one agency did not provide comments.

Of the 13 agencies that agreed with our recommendations 9 provided written comments which are reprinted in Appendix II, and 4 provided comments via email:

- In an email from its GAO/OIG Liaison, Commerce agreed with our recommendations and stated that it will prepare a formal action plan upon issuance of our report.

- In written comments, Education agreed with our recommendation and stated that they would endeavor to fully identify actors within their IT environment. Education also provided technical comments which we incorporated as appropriate.

- In written comments, Energy agreed with our recommendation and stated that the department has a project underway that will result in the inclusion of non-person entities within their records that is expected to run through December 2028.

- In written comments, HHS agreed with our recommendations and provided plans to implement them. Specifically, HHS plans to develop an actionable enterprise-wide zero trust plan that includes an inventory of actors and an inventory of assets by the end of quarter 2 of Fiscal Year 2027. It also plans to continue with enterprise-wide maturity of zero trust and to document roles and responsibilities and its implementation process as it continues.

- In written comments, DHS agreed with our recommendation and described plans to establish and apply a standardized assessment process for its high-value assets based on CISA's Zero Trust Maturity Model. DHS also provided technical comments which we incorporated as appropriate.

- In an email from its Audit Liaison Officer in its Office of the Chief Information Officer, HUD provided comments in an email stating that it agreed with our recommendations and included a description of how it plans to address them.

- In an email from an Audit Liaison Officer, DOJ agreed with our recommendation and stated that it had no comments.

- In written comments, State agreed with our recommendations and stated that it plans to implement them.

- In written comments, Treasury agreed with our recommendations and stated that it plans to implement them.

- In written comments, EPA agreed with our recommendations and stated that it plans to continue to update its plan for implementing ZTA to fully identify actors within its IT environment, and to formally document project management roles and responsibilities for its efforts.

- In written comments, NASA agreed with our recommendation and stated that it plans to work with its information system owners to score each of its affected systems via a scorecard instrument in accordance with the CISA Zero Trust Maturity Model.

- In an email from an Audit Liaison, NSF stated that it agreed with our report finding and had no comments.

- In written comments, OPM agreed with our recommendations and described plans to implement them. Specifically, it stated that the agency uses its Master User Record and the Continuous Diagnostics and Mitigation platform to manage person and non-person entities within its environment. OPM further explained that it leverages a Master Device Record to aggregate continuous inventory information. It also stated that it views zero trust as a continuing operational process, and that it plans to operate and extent its zero trust architecture beyond milestones from OMB's M-22-09 guidance. In addition, OPM described roles and responsibilities in place across the agency that support its zero trust efforts.

Of the four agencies that neither agreed nor disagreed with our recommendations:

- In an email from its OCIO Audit Liaison Officer, USDA stated that it did not have comments on our draft report.

- In an email from a Financial Specialist, Interior acknowledged receipt and review of the draft report and stated that it had no comments.

- In written comments reprinted in Appendix II, NRC stated that it had already addressed the two recommendations we made and provided supporting documentation for the actions it had taken. We reviewed this documentation and verified that the actions taken by the agency fully addressed our two recommendations. We plan to close recommendations 33 and 34 after we issue our report.

- In an email from its GAO Liaison, SBA stated that the agency has addressed all relevant NIST guidance and is working to address relevant OMB guidance.

Of the six agencies to which we did not make recommendations, five agencies—Labor, DOT, VA, GSA, SSA—responded that they had no comments on the report. OMB did not provide comments on the report.

How GAO Did This Study

In conducting this engagement, we reviewed 22 of the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies,[28] in order to obtain a view of zero trust across the federal government. In addition, we included the DHS's CISA, OMB, and Commerce's NIST. We did so because of the roles that CISA and NIST have in developing guidance for agencies to follow

concerning zero trust, and the role that OMB has in setting requirements for agencies concerning zero trust.

To address our objective, we assessed plans to implement zero trust architecture from the 22 selected civilian CFO Act agencies. To do so, we compared elements within the plans to selected guidance from OMB and NIST, respectively. Specifically, we compared the plan elements to 2024 guidance from an OMB memorandum,[29] 2020 guidance from NIST on zero trust architecture,[30] and 2003 guidance from NIST on IT security services.[31] The NIST guidance on IT security services provides practices that organizations can use to more effectively implement IT security projects; such projects could include ZTA.

We selected the OMB memorandum to assess the agencies' plans because the memorandum provided guidance that agencies were expected to implement concerning zero trust.[32] In addition, the memorandum leveraged guidance from CISA in implementing zero trust.[33]

Further, we selected NIST guidance based on relevance to zero trust efforts and IT project planning. Specifically, agencies have been required to plan for, and begin implementing, zero trust principles since 2021. Therefore, we selected NIST guidance that would be relevant to agency zero trust planning efforts given that zero trust implementation is ongoing.[34] In addition, since federal agencies' move to zero trust will require complex IT project management, we selected NIST guidance associated with managing the implementation of IT security services.

We interviewed cognizant cybersecurity officials from the 22 selected agencies to better understand their zero trust planning efforts. We also interviewed officials from CISA and NIST to better understand the guidance they developed. Although officials from OMB confirmed receipt of a notification letter we sent to the agency, officials did not respond to requests for an interview or respond to written questions.

We conducted this performance audit from July 2025 to November 2026 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.

List of Addressees

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

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

We are sending copies of this report to the appropriate congressional committees; the heads of the 22 selected civilian CFO Act agencies; the Director of the Cybersecurity and Infrastructure Security Agency; the Director of the National Institute of Standards and Technology; the Director of OMB; the Inspectors General of the 22 agencies; and other interested parties.

Staff Acknowledgments

This performance audit was completed under the direction of

David B. Hinchman
Director, Information Technology and Cybersecurity

Jennifer R. Franks
Acting Chief Technology Officer
Director, Center for Enhanced Cybersecurity

Other key contributors to this report were Tammi Kalugdan, Jeffrey Knott (Assistant Directors); Kevin Smith (Analyst-in-Charge), Tasha Beyzavi, Donna Epler, Smith Julmisse, Walter Vance, and Edward Varty made key contributions to this report.

APPENDIX I

Extent to Which Selected Agencies Addressed Requirements and Guidance

As discussed in our report, the Office of Management and Budget (OMB) developed requirements for agencies to follow concerning their zero trust architecture implementation plans in Memorandum M-24-14.[35] In addition, the National Institute of Standards and Technology (NIST) developed guidance for agencies concerning zero trust architecture in Special Publication 800-207.[36] NIST also developed guidance for agencies concerning information technology (IT) security services in Special Publication 800-35.[37] Table 2 shows the extent to which the selected 22 civilian Chief Financial Officers Act of 1990 agencies had addressed OMB requirements in their zero trust implementation plans as of August 2026.[38] Table 3 shows the extent to which the agencies had addressed NIST guidance in those plans.

Table 2: Extent to Which Selected Agencies Addressed Guidance from the Office of Management and Budget in Their Zero Trust Implementation Plans as of August 2026

Agency	Implement zero trust on all information systems	Assess maturity of high-value assets and high-impact systems
Department of Agriculture	●	○
Department of Commerce	●	○
Department of Education	●	●
Department of Energy	●	●
Department of Health and Human Services	○	●
Department of Homeland Security	●	◐
Department of Housing and Urban Development	●	●
Department of the Interior	●	◐
Department of Justice	●	◐
Department of Labor	●	●
Department of State	●	◐
Department of Transportation	●	●
Department of the Treasury	●	◐
Department of Veterans Affairs	●	●
Environmental Protection Agency	●	●
General Services Administration	●	●
National Aeronautics and Space Administration	◐	◐

Agency	Implement zero trust on all information systems	Assess maturity of high-value assets and high-impact systems
National Science Foundation	●	●
Nuclear Regulatory Commission	●	●
Office of Personnel Management	●	●
Small Business Administration	●	○
Social Security Administration	●	●

● Fully addressed

◐ Partially addressed

○ Not addressed

Source: GAO assessment of selected civilian Chief Financial Officers Act agency zero trust implementation plan documentation. | GAO-27-108661

Table 3: Extent to Which Selected Agencies Addressed Guidance from the National Institute of Standards and Technology in Their Zero Trust Implementation Plans as of August 2026

Agency	Identification of actors	Identification of assets	Expansion of the zero trust architecture	Project management roles and responsibilities	Implementation process
Department of Agriculture	◐	●	●	●	●
Department of Commerce	●	●	◐	○	◐
Department of Education	◐	●	●	●	●
Department of Energy	◐	●	●	●	●
Department of Health and Human Services	◐	◐	○	○	○
Department of Homeland Security	●	●	●	●	●
Department of Housing and Urban Development	◐	◐	●	●	◐
Department of the Interior	◐	●	◐	○	●
Department of Justice	●	●	●	●	●
Department of Labor	●	●	●	●	●

Agency	Identification of actors	Identification of assets	Expansion of the zero trust architecture	Project management roles and responsibilities	Implementation process
Department of State	◐	●	●	◐	●
Department of Transportation	●	●	●	●	●
Department of the Treasury	◐	●	●	○	●
Department of Veterans Affairs	●	●	●	●	●
Environmental Protection Agency	◐	●	●	◐	●
General Services Administration	●	●	●	●	●
National Aeronautics and Space Administration	●	●	●	●	●
National Science Foundation	●	●	●	◐	●
Nuclear Regulatory Commission	◐	●	●	○	●
Office of Personnel Management	◐	◐	◐	◐	●
Small Business Administration	●	●	●	●	●
Social Security Administration	●	●	●	●	●

● Fully addressed

◐ Partially addressed

○ Not addressed

Source: GAO assessment of selected civilian Chief Financial Officers Act agency zero trust implementation plan documentation. | GAO-27-108661

APPENDIX II

Comments from Agencies

Comments from Department of Education

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF THE CHIEF INFORMATION OFFICER

October 6, 2026

Mr. David Hinchman
Director, Information Technology and Cybersecurity
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hinchman:

Pursuant to 31 U.S.C. § 720, I am writing to provide the U.S. Department of Education's (Department's) response to the Government Accountability Office's (GAO's) draft report, *CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans (GAO-27-108661).* The Department understands that GAO conducted this audit to review the Department's implementation of Zero Trust Architecture (ZTA). The Department appreciates the opportunity to respond to the GAO recommendation set forth in the draft report. The recommendation and the Department's response are provided below.

GAO Recommendation 7: The Secretary of Education should ensure that the Department's Chief Information Officer updates the Department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment.

Response: The Department concurs with the recommendation and will endeavor to fully identify actors within the IT environment.

You may direct your questions to Mr. Walter McDonald, Chief Information Security Officer at 202-245-6794 or at Walter.McDonald@ed.gov (cc: Roman.Kulbashny@ed.gov and PQCrypto@ed.gov.)

Sincerely,

RAY CRAWFORD
Digitally signed by RAY CRAWFORD
Date: 2026.10.06 11:39:49 -04'00'

Ray Crawford
Acting Chief Information Officer

Comments from Department of Energy

Department of Energy
Washington, DC 20585

September 29, 2026

David Hinchman
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street N.W.
Washington, DC 20548

Dear Mr. Hinchman:

The Department of Energy (DOE or Department) appreciates the opportunity to comment on the Government Accountability Office's (GAO) draft report titled, "*Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans.*" DOE provides the following comments below.

The draft report contains a total of forty (40) recommendations, of which GAO directed one (1) recommendation to DOE. DOE concurs with GAO's recommendation. The Department has a project underway that will result in the inclusion of non-person entities within their records, which was noted in the GAO report. This project is expected to run through December 2028, and upon completion of the initiative we will update our ZT Implementation documentation to account for this service.

GAO should direct any questions to Robert Knisely, Chief Information Security Officer, in the Office of Chief Information Officer via Robert.Knisely@hq.doe.gov.

Sincerely,

DAWN ZIMMER
Digitally signed by DAWN ZIMMER
Date: 2026.09.28 11:07:40 -04'00'

Dawn Zimmer
Chief Information Officer

Enclosure

Enclosure

Management Response
GAO Draft Report: ***Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans*** **(GAO-27-108661)**

Recommendation 8: The Secretary of Energy should ensure that the department's Chief Information Officer updates its zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice of identifying actors within its IT environment.

DOE Response: Concur

The Department has a project underway that will result in the inclusion of non-person entities within their records, which will implement the guidance cited in the GAO report for identifying actors within the IT environment. This project is expected to run through December 2028, and upon completion of the initiative we will update our zero trust implementation documentation to account for this service.

Estimated Completion Date: December 2028

Comments from Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES — OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

October 6, 2026

David Hinchman
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Jennifer R. Franks
Acting Chief Technology Officer
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman and Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans"** (GAO-27-108661).

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

Sincerely,

Gary Andres
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CYBERSECURITY: AGENCIES NEED TO FULLY ADDRESS FEDERAL GUIDANCE AS THEY REFINE ZERO TRUST ARCHITECTURE PLANS (GAO-27-108661)

The Department appreciates the opportunity to review and comment on this draft report.

GAO Recommendation 9
The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully documents an enterprise-wide implementation plan for zero trust architecture that incorporates guidance from the Office of Management and Budget.

HHS Response
HHS concurs with GAO's recommendation and will prioritize this effort at the conclusion of our current Zero-Trust (ZT) Maturity Scorecard data call, which will be finalized by the end of Fiscal Year 2026 (FY26). HHS has already reached out to the Cybersecurity and Infrastructure Security Agency (CISA) ZT Community of Practice and other ZT teams across the Federal Civilian Executive Branch (FCEB) to inquire about documentation other agencies are willing to share that HHS may leverage as helpful concepts to include in the implementation plan. HHS will solicit input from Divisions through the enterprise-wide Zero Trust Working Group and strive to make the plan as actionable as possible based on the progress already achieved across the Department. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

GAO Recommendation 10
The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment as it documents its enterprise-wide plan.

HHS Response
HHS concurs with GAO's recommendation and will document the capabilities for establishing a comprehensive inventory of every actor within HHS' IT environment in the enterprise-wide implementation plan for zero trust architecture. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

GAO Recommendation 11
The Secretary of Health and Human Servies should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of identifying assets within its IT environment as it documents its enterprise-wide plan.

HHS Response
HHS concurs with GAO's recommendation and will document the capabilities for establishing a comprehensive inventory of every asset within HHS' IT environment in the enterprise-wide implementation plan for zero trust architecture. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

GAO Recommendation 12
The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture in documenting the department's enterprise-wide plan.

HHS Response
HHS concurs with GAO's recommendation and will document HHS' plans to continue with enterprise maturity within the enterprise-wide implementation plan for zero trust architecture. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

GAO Recommendation 13
The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts in documenting the department's enterprise-wide plan.

HHS Response
HHS concurs with GAO's recommendation and will document roles and responsibilities for zero trust efforts within the enterprise-wide implementation plan for zero trust architecture. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

GAO Recommendation 14
The Secretary of Health and Human Services should ensure that the department's Chief Information Officer fully addresses the National Institute of Standards and Technology practice to document the implementation process as it documents its enterprise-wide plan.

HHS Response
HHS concurs with GAO's recommendation and will document HHS' implementation process within the enterprise-wide implementation plan for zero trust architecture. HHS expects this document to be ready to be shared by the end of Quarter 2 of Fiscal Year 2027.

Comments from Department of Homeland Security

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

Homeland Security

BY ELECTRONIC SUBMISSION

October 2, 2026

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

Jennifer R. Franks
Acting Chief Technology Officer
Director, Center for Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-27-108661 "CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans"

Dear Mr. Hinchman and Ms. Franks:

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

DHS leadership is pleased to note GAO's recognition that the Department fully addressed guidance from the Office of Management and Budget (OMB) in the plan to implement Zero Trust Architecture (ZTA) on all information systems, and that DHS made progress to implement OMB guidance in the assessment of maturity of high value assets and high-impact systems. The Department's ZTA implementation plan is comprehensive, and encompasses all DHS information systems. Furthermore, DHS established and documented clear procedures to identify actors and assets within our complex information technology environment. DHS remains committed to fully transitioning to

ZTA in alignment with federal guidance, ensuring that the Department verifies everything that attempts to access DHS systems and services.

The draft report contained 40 recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration, as appropriate.

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,

DAVID E SCHMITT
Digitally signed by DAVID E SCHMITT
Date: 2026.10.02 13:34:44 -04'00'

DAVID SCHMITT
Director
Departmental Audit Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-27-108661

GAO recommended that the Secretary of Homeland Security:

Recommendation 15: Ensure that the department's Chief Information Officer fully documents the maturity levels for all of its high-value assets and high-impact systems based on the zero-trust maturity model developed by the Cybersecurity and Infrastructure Security Agency [CISA].

Response: Concur. The DHS Office of the Chief Information Officer (OCIO), through the Office of the Chief Information Security Officer (OCISO), will establish and apply a standardized assessment and documentation process based on the CISA Zero Trust Maturity Model. The OCISO will reconcile the assessment population against the Departments' authoritative inventories to ensure that all identified high-value asset information systems and high-impact systems are included.

For each system, the Department will document the assessed maturity level across the applicable Zero Trust pillars and cross-cutting capabilities, the evidence supporting each determination, identified gaps, and the responsible reviewing and approving officials. The completed assessments will be maintained in a centralized repository and periodically reviewed and updated to reflect material changes to system architecture, security controls, CISA guidance, or asset designation.

The assessment results will provide a Department-wide maturity baseline and support risk-informed remediation, resource allocation, and investment priorities for implementing ZTA. Estimated Completion Date: September 30, 2027.

0

Comments from Department of State

United States Department of State

Washington, DC 20520

OCT 14 2026

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

Dear Ms. Gianopoulos:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans." GAO Job Code 108661.

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

Sincerely,

Mark Erickson
Deputy Executive Director
Office of the Under Secretary for Management
Under Secretary for Management Executive Office

Enclosure:
As stated

cc: GAO – Jennifer Franks
OIG - Norman Brown

Department of State Comments to GAO Draft Report

CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans
(GAO-27-108661, GAO Code 108661)

The Department of State appreciates the opportunity to review the GAO draft report, *"Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans."*

Recommendation 24: The Secretary of State should ensure that the Department Chief Information Officer documents the maturity levels for all of its high value assets and high impact systems based on the zero-trust maturity model developed by the Cybersecurity and infrastructure Security Agency.

Response: The Department concurs with the recommendation. The Chief Information Officer (CIO) will ensure that documented maturity levels are established for all high value assets (HVAs) and high impact systems in alignment with the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model. The Department will continue strengthening its zero-trust architecture and related assessment processes.

Recommendation 25: The Secretary of State should ensure that the Department Chief Information Officer updates the department's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment.

Response: The Department concurs with the recommendation. The CIO will update the Department's Zero Trust Architecture Implementation Plan to fully incorporate the National Institute of Standards and Technology (NIST) zero-trust migration requirement for identifying actors within the Department's IT environment. This enhancement will support more robust identity management, strengthen access controls, and advance the Department's broader zero-trust modernization efforts.

Recommendation 26: The Secretary of State should ensure that the department's Chief Information Officer updates the department's zero trust architecture

implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts.

Response: The Department concurs with the recommendation. The CIO will update the Department's Zero Trust Architecture Implementation Plan to fully align with the National Institute of Standards and Technology (NIST) practice of documenting roles and responsibilities for all zero-trust activities. This update will help ensure clearer accountability, strengthen governance, and support more effective implementation of the Department's zero-trust strategy.

Comments from Department of Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 16, 2026

David Hinchman
Director, Information Technology and Cybersecurity
General Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Hinchman:

Thank you for the opportunity to review GAO's draft report entitled "Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans" (Draft Report). The Department of the Treasury remains committed to advancing Zero Trust Architecture (ZTA) across its information technology environment and appreciates GAO's assessment of agency implementation planning against federal guidance.

Treasury appreciates GAO's recognition that its ZTA implementation plan covers all information systems and fully addresses the identification of enterprise assets, expansion of zero trust architecture, and the implementation process. These elements provide a foundation for continued modernization and coordination across Treasury components. The Draft Report contains three recommendations for Treasury, and we address each in turn below.

Recommendation 27: We agree with GAO's recommendation that the Secretary of the Treasury ensure that Treasury's Chief Information Officer (CIO) fully document the maturity levels of all of its high-value assets and high-impact systems based on the zero trust maturity model developed by the Cybersecurity and Infrastructure Security Agency (CISA). Treasury will review the completeness of its documentation, coordinate with responsible system owners to address missing or outdated entries, and assess improvements to reporting and validation against the CISA Zero Trust Maturity Model.

Recommendation 28: We agree with GAO's recommendation that the Secretary of the Treasury ensure that the CIO update Treasury's plan to implement ZTA to fully address the National Institute of Standard and Technology (NIST) zero trust migration step of fully identifying actors within its IT environment. Treasury will review and update its planning documentation to describe how these actors are identified and managed across the enterprise, consistent with NIST SP 800-207.

Recommendation 29: We agree with GAO's recommendation that the Secretary of the Treasury ensure that the CIO update Treasury's plan to implement ZTA to fully address the NIST practice to document roles and responsibilities for its zero trust architecture.

Treasury Response: Treasury acknowledges GAO's finding that its implementation plan did not define ZTA project management roles and responsibilities at the component level. Treasury will work with relevant departmental and component stakeholders to clarify and document

responsibilities for ZTA planning, implementation, coordination, and ongoing operations, consistent with NIST SP 800-35.

Treasury remains committed to strengthening enterprise-wide visibility, accountability, and sustained implementation of zero trust principals. Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

Respectfully,

Samuel J. Corcos

Digitally signed by Samuel J. Corcos
Date: 2026.10.30 09:40:00 -04'00'

Samuel Corcos
Deputy Assistant Secretary for Information Technology and Chief Information Officer
U.S. Department of the Treasury

Comments from Environmental Protection Agency

OFFICE OF FINANCE AND ADMINISTRATION
WASHINGTON, D.C. 20460

October 6, 2026

Mr. David Hinchman
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Hinchman:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's draft report, *"Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans"* (GAO-27-108661). The U.S. Environmental Protection Agency sincerely values GAO's ongoing collaboration and partnership, which has greatly contributed to advancing the agency's zero trust efforts. GAO's feedback is essential to our improvement initiatives, and EPA appreciates the insights provided throughout this engagement.

This letter provides EPA's response to the draft report's findings, conclusions and recommendations. The agency agrees with GAO's conclusions and recommendations and would like to share recent progress and next steps regarding the agency's Zero Trust Architecture efforts, as guided by the National Institute of Standards and Technology.

The GAO determined that the adoption of ZTA principles is vital for ensuring the security of information and systems. Considering ongoing technological advancements, the continued development and assessment of zero trust solutions are imperative, and implementation strategies must adapt to address evolving security threats. To facilitate progress in this area, the GAO issued two recommendations. The EPA recognizes the importance of continuous improvement and is implementing the corrective action plans described below to address the recommendations.

GAO Recommendation #30:
The Administrator of the Environmental Protection Agency should ensure that the agency's Chief Information Officer updates the agency's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of fully identifying actors within its IT environment.

EPA Response:
EPA agrees with this recommendation. The agency's Zero Trust team has successfully identified both standard and privileged users throughout the enterprise. However, gaps remain regarding service accounts and Non-Person Entities. Established workflows are in place for the requesting, approval, and onboarding of service accounts. During FY26, the Zero Trust team fully identified and classified service accounts and established procedures to automate the cleanup of inactive or stale service accounts. EPA will continue to update its plan for implementing zero trust architecture to ensure comprehensive alignment with the NIST zero trust migration step, specifically by fully identifying all actors within its information technology environment.

GAO Recommendation #31:
The Administrator of the Environmental Protection Agency should ensure that the agency's Chief Information Officer updates the agency's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology practice of documenting project management roles and responsibilities for its zero trust efforts.

EPA Response:
EPA agrees with this recommendation. The agency's Zero Trust team is presently composed of a dedicated project manager and five ZTA Pillar Leads for Identity, Device, Network, Application and Data, each tasked with overseeing the implementation of zero trust practices within their respective domain. EPA will formally document the project management roles and responsibilities for its zero trust efforts.

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

Sincerely,

C. Paige Hanson

C. Paige Hanson
Chief Financial Officer and
Chief Administrative Officer
U.S. Environmental Protection Agency

cc: Gregg Treml, OFA
Jennie Campbell, OFA
Tonya Manning, OFA
Fletcher Mutz, OFA
Lek Kadeli, OFA
Sylvana, Li, OFA
David Alvarado, OFA
Owen Handle, OFA
Kevin Ruano, OFA
Lee Kelly, OFA

Douglas Vick, OFA
Tommy Sant'Agata, OFA
Kaitlyn Khan, OFA
Nancy Broom, OFA
Mack Zakikhani, OFA
Tyler Rubright, OFA
Jan Jablonski, OFA
Afreeka Wilson, OFA
Sara Elkassabany, OFA
Kevin Haywood, OFA
Tracey Monroe, OFA
OFA Audit Coordination
Andrew LeBlanc, OFA
EPA GAO Liaison Team
Kristien Knapp, OCIR
Joanne Thomas, OGC

Comments from National Aeronautics and Space Administration

National Aeronautics and Space Administration

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

Reply to Attn of: Office of the Chief Information Officer

David Hinchman
Director
Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hinchman:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans" (GAO-27-108661), dated September 8, 2026.

In this draft report, GAO found 17 agencies had not fully addressed guidance from the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) in their zero trust architecture planning.

GAO makes one recommendation addressed to the NASA Administrator. Specifically, GAO recommends the following:

Recommendation 32: The Administrator of NASA should ensure that the administration's Chief Information Officer (CIO) fully documents the maturity levels of its high-value assets and high-impact systems based on the Zero Trust Maturity Model (ZTMM) developed by the Cybersecurity and Infrastructure Security Agency (CISA).

Management's Response: NASA concurs with this recommendation.

The NASA CIO, through its Cybersecurity Improvements Portfolio Core Team, will work with the Agency's 35 High Value Assets' (HVA) and 49 Federal Information Security Modernization Act (FISMA) High systems' Information Systems Owners and Information Systems Security Officers to score each of the affected systems via a scorecard instrument in accordance with the CISA ZTMM Version 2.0. The HVA and FISMA High systems scores will then be consolidated into separate tables, detailing each system's identification number, authorization package name, government owned/contractor operated status (yes/no), Software as a Service cloud offering (yes/no), and current and target Zero Trust Maturity levels with any associated notes broken out by pillars (Identity, Devices, Networks, Applications/Workloads, and Data). These tables will be made part of an update to the Federal CIO with a copy to CISA.

Estimated Completion Date: 03/26/2027

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

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

Sincerely,

Sean Gallagher Digitally signed by Sean Gallagher
Date: 2026.10.15 12:26:52 -04'00'

Sean Gallagher
Chief Information Officer

Comments from Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

October 6, 2026

David Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

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

Dear Director Hinchman and Director Franks:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans, GAO-27-108661, GAO job code 108661.

The U.S. Office of Personnel Management (OPM) concurs with all four recommendations directed to OPM and remains committed to advancing its zero trust architecture (ZTA) to secure its information technology (IT) environment. Responses to your recommendations are provided below.

Recommendation 36: The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment.

Management Response: We concur.

Consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 §7.3.1, OPM identifies as enterprise subjects both person entities and non-person entities, including service accounts and privileged administrative accounts, together with the privileges assigned to them.

The Master User Record (MUR) is OPM's procedure for identifying person entities. OPM's corresponding procedure for identifying non-person entities operates through its Continuous Diagnostics and Mitigation (CDM)-funded enterprise asset discovery and inventory platform. This platform integrates directly with the enterprise directory, enumerates accounts on a recurring automated cycle, classifies each account as person or non-person by its directory placement rather than by naming convention, and records its directory group memberships.

Accounts assigned privileged administrative roles are held in a dedicated directory location and are identified by that placement, ensuring they receive additional scrutiny when attributes or roles are assigned. Access behavior by both person and non-person subjects is recorded in

OPM's enterprise security monitoring platform and evaluated through behavioral analytics, so that access patterns for privileged and automated accounts can be continuously reviewed.

These capabilities align with the following NIST SP 800-53 Revision 5 controls: IA-4 (Identifier Management), IA-5 (Authenticator Management), AC-2 (Account Management), AC-3 (Access Enforcement), AC-6 (Least Privilege), and AU-6 (Audit Record Review, Analysis, and Reporting).

Recommendation 37: The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying assets within its IT environment.

Management Response: We concur.

Consistent with NIST SP 800-207 §7.3.2, OPM's procedure for identifying assets extends beyond cataloging and maintaining a database of assets to include the configuration management and monitoring of those assets.

The Master Device Record (MDR) is assembled from OPM's reconciled enterprise asset inventory, which aggregates and deduplicates device records from eight authoritative sources across the on-premises and cloud environments and records each asset's network location. Because a complete census of enterprise assets cannot be assumed, the inventory procedure is continuous rather than periodic: newly observed assets are discovered, categorized, and risk-assessed automatically. Assets that are not enterprise-managed, including devices present on enterprise network infrastructure that are not centrally managed, are cataloged through network access control monitoring to the extent they are visible to the enterprise.

Configuration of enterprise assets is managed through three mechanisms. Group Policy applies Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) baselines across the enterprise Windows estate. Enterprise endpoint management holds the security baselines, configuration profiles, and compliance policies assigned to managed endpoints, including virtual desktop and cloud-hosted assets. Cloud configuration policy establishes and enforces policies for other cloud resource types.

Least-functionality controls are enforced on endpoints through attack surface reduction policy. Endpoint and cloud compliance state is evaluated on a recurring automated cycle, and endpoint compliance state is supplied to the enterprise identity platform as a device signal in conditional access decisions. Changes to asset configuration and to the enterprise baselines are governed through OPM's Enterprise Change Management process, which requires an approval record and a security impact analysis.

These capabilities align with the following NIST SP 800-53 Revision 5 controls: CM-2 (Baseline Configuration), CM-3 (Configuration Change Control), CM-6 (Configuration Settings), CM-7 (Least Functionality), CM-8 (Information System Component Inventory), CA-7 (Continuous Monitoring), and IA-3 (Device Identification and Authentication).

Recommendation 38: The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's plan to implement zero trust

architecture to fully address the National Institute of Standards and Technology zero trust migration step of expanding the zero trust architecture.

Management Response: We concur.

Consistent with NIST SP 800-207 §7.3.7, OPM treats zero trust as a continuing operational process, not a program with a completion date. The Office of Management and Budget (OMB) Memorandum M-22-09 milestones represent initial deployment; the procedures below describe how OPM operates and extends the architecture beyond that phase.

Once a workflow's policy set is refined and operating as intended, the workflow enters a steady operational phase: assets and traffic remain monitored and logged, and policy is adjusted at a lower tempo. The subjects and stakeholders of the resources and processes involved provide feedback to improve operations. OPM's Zero Trust Governance Team is accountable for obtaining that feedback and reviewing implementation progress and pillar maturity. OPM will re-establish the team, establish a recurring review cadence, and consolidate the data pillar working group and its Data Governance Board coordination under the team so that pillar feedback reaches one body.

OPM is extending the architecture to the Data pillar through an enterprise data classification and sensitivity labeling effort now in development, with a parallel data loss prevention re-architecture. Together, these efforts are determining the sensitivity label taxonomy that data-centric policy depends on, testing automated classifiers against enterprise content, and developing the custom sensitive information types that policy requires. Limited-scope attribute-based access control and a pilot with data stewards from the affected program offices are planned as later increments, with pilot feedback informing label design and policy thresholds before enterprise enforcement.

While a workflow is operational, OPM plans the next deployment phase, identifying the next candidate workflow and solution set and developing initial policies for it. Each new policy set is ordinarily first operated against a pilot scope in observation and reporting-only mode, establishing baseline access behavior and confirming that the policy is workable before promotion to enforcement and expansion. Controls whose failure conditions are unambiguous, such as requests that fail multifactor authentication or originate from known malicious infrastructure, are enforced from initial deployment.

Expansion is iterative. A significant change may alter a workflow or its policies, such as new devices, a major software update (particularly to software supporting zero trust logical components), or a shift in organizational structure. Where that occurs, the architecture for the affected scope is reevaluated and the process reconsidered on the assumption that some work is already done.

Recommendation 39: The Director of the Office of Personnel Management should ensure that the office's Chief Information Officer updates the office's zero trust architecture

implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts.

Management Response: We concur.

Consistent with the practice in NIST SP 800-35 §4.3.3 of identifying the roles and responsibilities of individuals with project management responsibilities for both the implementation and operations phases, OPM documents the roles and responsibilities assigned to its zero trust effort. Responsibilities are assigned by role. The Chief Information Officer and Chief Information Security Officer responsibilities below are recorded in OPM's Cybersecurity and Privacy Policy and are reproduced here as they apply to this plan.

Chief Information Officer. Reviews and approves the zero trust strategy, secures funding, and aligns the initiative with business goals during the implementation phase. Reviews and provides input on maturity metrics and risk compliance, and reports progress to leadership and external entities as necessary, during the operational phase.

Chief Information Security Officer. Formulates and approves the zero trust strategy, aligns the initiative with business goals, coordinates cross-functional teams, and tracks project milestones during the implementation phase. Sets maturity goals, defines key metrics, and monitors outputs for continuous improvement during the operational phase. Reports progress to leadership and external entities as necessary.

Zero Trust Governance Team. The cross-functional body accountable for coordinating the zero trust effort across the pillars, composed of Associate Chief Information Officers and director-level staff from the product, platform, and cybersecurity organizations. During implementation, the team coordinates activities across pillars and reviews progress against the zero trust roadmap. During operations, it reviews pillar maturity reassessment results and feedback from participating program offices. The team partners with OPM's Enterprise Program Management Office for reporting on progress, risks and issues, procurement-related activities, and resource topics.

Pillar leads. A lead is designated for each zero trust pillar and for the cross-cutting capabilities of visibility and analytics, automation and orchestration, and governance. The Network Engineering Branch Chief leads the Networks pillar; security engineers within the Office of the Chief Information Security Officer lead the Identity, Devices, Applications and Workloads, and Data pillars; and the Security Engineering Team Lead holds the cross-cutting capabilities. During implementation, each lead drives the implementation activities and maturity assessment within that pillar and is consulted on changes affecting adjacent pillars. During operations, each lead monitors pillar state, reports status to the Zero Trust Governance Team, and identifies candidate workflows for the next expansion increment.

Zero trust sponsor, per system. Each system brought under the zero trust architecture has a designated sponsor accountable for implementation within that system's boundary, currently the system's Information System Security Engineer. During implementation, the sponsor coordinates the system's participation in the applicable expansion increment and supplies the system information that sequencing decisions depend on. During operations, the sponsor is the point of accountability for the system's zero trust posture and reports exceptions to the responsible pillar lead.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Andrew Hopkins, Director, Office of Legislative Affairs, at Andrew.Hopkins@opm.gov.

Sincerely,

ADAM STARR Digitally signed by ADAM STARR
Date: 2026.10.05 18:01:36 -04'00'

Adam Starr
Senior Advisor to the Director, Performing the Duties of the Chief Information Officer
U.S. Office of Personnel Management

Comments from Nuclear Regulatory Commission

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

October 08, 2026

David Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20226

Dear Director Hinchman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to the U.S. Government Accountability Office (GAO) Draft Report: Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans (GAO-27-108661), sent via email on September 8, 2026. The NRC appreciates the opportunity to review the report. The NRC focused our review on sections applicable to us and enclosed are our comments for the draft report. As evidence supporting the NRC's response to recommendation 34, see the updated Nuclear Regulatory Commission Zero Trust Strategy Implementation Plan (Agencywide Documents Access and Management System (ADAMS) Accession No. ML26275A127). If you have any questions or need additional information, please contact me or have your staff contact Erin Deeds by via e-mail at Erin.Deeds@nrc.gov.

Sincerely,

Signed by Caroline Carusone Signing on behalf of Mike King on 10/08/26

Michael F. King
Executive Director
for Operations

Enclosure:
As stated

SUBJECT: RESPONSE TO DRAFT REPORT - CYBERSECURITY: AGENCIES NEED TO FULLY ADDRESS FEDERAL GUIDANCE AS THEY REFINE ZERO TRUST ARCHITECTURE PLANS (GAO-27-108661) DATED: XX/XX/XXXX

DISTRIBUTION:
RidsEdoMailCenter Resource
EDeeds, OEDO

ADAMS Accession Numbers: Pkg: ML26272A148; Letter: ML26272A158;
SCD: ML26272A159

NRC Response to Draft Report: Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans (GAO-27-108661)

1. GAO Recommendation 33: On page 27, GAO recommends that "The Chairman of the Nuclear Regulatory Commission should ensure that the commission's Chief Information Officer updates the commission's plan to implement zero trust architecture to fully address the National Institute of Standards and Technology zero trust migration step of identifying actors within its IT environment."

   NRC Response: The NRC Zero Trust Implementation has been updated to include additional details related to the migration step of identifying actors within its IT environment. The updated plan will be provided to GAO shortly to address this recommendation.

2. GAO Recommendation 34: On page 20, the draft report states that NRC "did not identify zero trust implementation roles and responsibilities within their ZTA planning documentation," and "did not explain why they had not addressed this element in their zero trust planning documentation."

   Recommendation 34 on page 28 recommends that "The Chairman of the Nuclear Regulatory Commission should ensure that the commission's Chief Information Officer updates the commission's zero trust architecture implementation plan to fully address the National Institute of Standards and Technology practice to document roles and responsibilities for its zero trust efforts."

   NRC Response: In 2026 communications with GAO auditors prior to issuance of the draft report, the NRC explained that zero trust implementation roles and responsibilities are clearly defined at the Agency and included in internal zero trust documentation, but that previous NRC Zero Trust Implementation Plan submissions to OMB did not list the specific names of the NRC ZTA implementation team members because this was not requested as part of the ZTA reporting template required for the submission. The NRC also explained that the official NRC Zero Trust Implementation Plan has been updated with the details of NRC staff who have been assigned roles and responsibilities for its zero trust efforts.

   Accordingly, the NRC requests that the draft report be updated and that recommendation 34 should reflect this status.

Enclosure

Comments from Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

David Hincham
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Hinchman,

Thank you for the opportunity to review the draft report "CYBERSECURITY: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans" (108661). We have no comments.

Please let me know if I can be of further assistance. Your staff may contact Amy Gao, Director of the Audit Liaison Staff.

Sincerely,

Chad Poist
Chief Risk Officer

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix III

References

Abbreviations

CFO Act	Chief Financial Officers Act of 1990
CISA	Cybersecurity and Infrastructure Security Agency
DOJ	Department of Justice
DOT	Department of Transportation
EPA	Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
HVA	high-value assets
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SBA	Small Business Administration
SSA	Social Security Administration
USDA	Department of Agriculture
VA	Veterans Affairs
ZTA	zero trust architecture

Citing This Report

This report should be cited as:

GAO, *Cybersecurity: Agencies Need to Fully Address Federal Guidance as They Refine Zero Trust Architecture Plans*, GAO-27-108661 (Washington, D.C.: November 18, 2026).

Copyright

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.

Endnotes

[1]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model,* Version 2.0 (Arlington, VA: April 2023).
[2]The 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), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.
[3]The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. For our engagement, we included only the civilian agencies in our review; we plan to review zero trust at the Department of Defense separately in the upcoming year. In addition, we did not include the U.S. Agency for International Development because the agency's functions are in the process of being incorporated into the Department of State. Therefore, the 22 civilian agencies covered in this review are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration.
[4]National Institute of Standards and Technology, *Zero Trust Architecture*, Special Publication 800-207 (Gaithersburg, MD: August 2020).
[5]National Institute of Standards and Technology, *Zero Trust Architecture*.
[6]National Institute of Standards and Technology, *Implementing a Zero Trust Architecture*, Special Publication 1800-35 (Gaithersburg, MD: June 2025).
[7]National Institute of Standards and Technology, *Guide to Information Technology Security Services*, Special Publication 800-35 (Gaithersburg, MD: October 2003).
[8]The White House, Improving the Nation's Cybersecurity, Executive Order 14028 (Washington, D.C.: May 12, 2021).
[9]Cybersecurity and Infrastructure Security Agency's *Zero Trust Maturity Model*. CISA previously issued Version 1.0 of this model in June 2021.
[10]According to the CISA model, the rating levels increase as an agency transitions towards optimal zero trust implementation. Associated solutions increasingly rely on automated processes, cross-pillar coordination, and dynamically-enforced policy decisions.
[11]Office of Management and Budget, *Federal Zero Trust Strategy*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

[12]The memorandum outlines actions that are to be taken by the end of fiscal year 2024. However, certain activities described in the memorandum have different timelines, including, for example, 1 year after publication of the memorandum, or based on agency implementation plans.
[13]Office of Management and Budget, *Administration Cybersecurity Priorities for the FY 26 Budget*.
[14]GAO, *Science & Tech Spotlight: Zero Trust Architecture,* GAO-23-106065 (Washington, D.C.: November 2022).
[15]GAO, *Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains*, GAO-23-105466 (Washington, D.C.: Nov. 15, 2022).
[16]Office of Management and Budget, *Administration Cybersecurity Priorities for the FY 26 Budget*.
[17]NASA Office of Inspector General, *Audit of NASA's Zero Trust Architecture,* IG-25-004 (Washington, D.C.: Mar. 27, 2025). Because the NASA Inspector General has already made a recommendation to address NASA's lack of an enterprise-wide ZTA plan, we are not making a recommendation to NASA in this regard. As of August 2026, the IG's recommendation had not been implemented.
[18]HHS is a federated agency and has 13 primary operating divisions including, for instance, the Food and Drug Administration and National Institutes of Health.
[19]High-value assets are those information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries. A high-impact system is one in which the loss of confidentiality, integrity, or availability of that system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
[20]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model.* As described earlier in the report, maturity levels include Traditional, Initial, Advanced, and Optimal and pillars include Identity, Devices, Network, Applications and Workloads, and Data.
[21]Cybersecurity and Infrastructure Security Agency, *Adapting Zero Trust Principles to Operational Technology* (Arlington, VA: April 2026).
[22]As described above, a policy engine is a component of a zero trust architecture that is responsible for the ultimate decision to grant access to a resource for a given subject.
[23]A non-person entity has a digital identity that acts in cyberspace but is not a human actor. This can include service accounts, organizations, hardware devices, software applications, and information artifacts.
[24]Although HHS had not developed a ZTA implementation plan that covered all of its information systems, they had documented some, but not all, elements for ZTA in separate documentation.
[25]The CDM program is intended to strengthen the cybersecurity of government networks and systems by providing tools to agencies to support continuous monitoring of their networks. The CDM program includes capabilities intended to help agencies identify cybersecurity risks on an ongoing basis, use CDM information to prioritize the risks based on potential impacts, and then mitigate the most significant vulnerabilities first. According to CISA's CDM data model, a master user record represents an entity (person or non-person) that requests access to information, information systems, and facilities.
[26]OMB considered requirements in its M-22-09 memorandum to be a starting point for zero trust implementation. OMB did not consider the requirements in M-22-09 to fully support zero trust, and its guidance states that full implementation would require additional efforts beyond those items in the memorandum.
[27]Office of Management and Budget, *Federal Zero Trust Strategy.*
[28]The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. For our engagement, we included only the civilian agencies in our review; we plan to review zero trust at the Department of Defense separately in the upcoming year. In addition, we did not include the U.S. Agency for International Development because

the agency's functions are in the process of being incorporated into the Department of State. Therefore, the 22 civilian agencies covered in this review are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration.

[29]Office of Management and Budget, *Administration Cybersecurity Priorities for the FY 26 Budget*, M-24-14 (Washington, D.C.: Jul. 10, 2024). This memorandum requires agencies to incorporate elements of the Cybersecurity and Infrastructure Security Agency's *Zero Trust Maturity Model*, version 2.0 (Arlington, VA: April 2023).

[30]National Institute of Standards and Technology, *Zero Trust Architecture*

[31]National Institute of Standards and Technology, *Guide to Information Technology Security Services*.

[32]OMB has published other guidance specific to zero trust, OMB M-22-09. See Office of Management and Budget, *Federal Zero Trust Strategy*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

[33]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model.*

[34]A 2021 Executive Order required that agencies plan for and begin adoption of zero trust principles. See: The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[35]Office of Management and Budget, *Administration Cybersecurity Priorities for the FY 26 Budget*

[36]National Institute of Standards and Technology, *Zero Trust Architecture*).

[37]National Institute of Standards and Technology, *Guide to Information Technology Security Services*

[38]The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. For our engagement, we included only the civilian agencies in our review; we plan to review zero trust at the Department of Defense separately in the upcoming year. In addition, we did not include the U.S. Agency for International Development because the agency's functions are in the process of being incorporated into the Department of State.

Appendix IV

Accessible Data for Figures

Accessible Data for Figure 3: The Cybersecurity and Infrastructure Security Agency's Five Pillars of Zero Trust Architecture

Pillar	Description
Identity	Enforcing access controls to confirm the identity of all users. Ensuring that the right users have the right access at the right time.
Devices	Compiling and maintaining ongoing inventories of all devices connected to the network. Ensuring that devices are secure to prevent, detect, and respond to unauthorized access to an enterprise's resources.
Networks	Encrypting open communication channels that are used to transport messages on the network. Segmenting those channels into isolated environments.
Applications and Workloads	Securing and managing applications by performing rigorous internal and external testing and decreasing reliance on network security.
Data	Protecting data on devices, networks, and applications by implementing enterprise-wide logging and information sharing.

Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model Version 2.0 and other relevant federal policies and guidance. | GAO-27-108661

Accessible Data for Figure 4: Extent to Which 22 Civilian Chief Financial Officers Act Agencies Addressed Selected Federal Guidance in Their Zero Trust Implementation Plans as of August 2026

Guidance document	Guidance	Addressed	Partially addressed	Not addressed
Office of Management and Budget Memorandum M-24-14 Guidance[a]	Covers implementation of zero trust on all information systems	20	1	1
	Documents the current zero trust maturity levels for all high value assets and high impact systems	13	6	3
National Institute of Standards and Technology Special Publication 800-207 Migration Steps[b]	Identifies actors on the enterprise	11	11	0
	Identifies assets owned by the enterprise	19	3	0
	Expands the zero trust architecture	18	3	1
National Institute of Standards and Technology Special Publication 800-35 Information Technology Planning Elements[c]	Addresses project management roles and responsibilities	13	4	5
	Addresses the implementation process	19	2	1

Source: GAO analysis of agencies' zero trust architecture implementation plans. | GAO-27-108661

[a]Office of Management and Budget, Administration Cybersecurity Priorities for the FY 26 Budget, M-24-14 (Washington, D.C.: Jul. 10, 2024). Requires agencies to incorporate into their zero trust planning elements of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model, version 2.0 (Arlington, VA: April 2023).

[b]National Institute of Standards and Technology, Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: August 2020).

[c]National Institute of Standards and Technology, Guide to Information Technology Security Services, Special Publication 800-35 (Gaithersburg, MD: October 2003).

About GAO

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, 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.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube. Subscribe to our 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:
https://www.gao.gov/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director,
Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director,
CongRel@gao.gov

General Inquiries

https://www.gao.gov/contact-us



Please Print on Recycled Paper.