United States Government Accountability Office

Report to Congressional Requesters

November 2022

CYBERSECURITY

Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains

Accessible Version

GAO-23-105466

GAO Highlights

Highlights of GAO-23-105466, a report to congressional requesters

November 2022

CYBERSECURITY

Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains

Why GAO Did This Study

Given the ever-increasing cyber threat landscape, the federal government has initiatives underway intended to protect agency IT. One such initiative, a zero trust architecture, is based on the concept that no actor operating outside or within an organization's network should be trusted.

The U.S. Secret Service, a component of the Department of Homeland Security (DHS), relies heavily on the use of IT to support its protection and financial investigations mission. GAO was asked to review cybersecurity at the agency. The objective of this report was to evaluate Secret Service's implementation of a zero trust architecture.

To do so, GAO reviewed the activities associated with four milestones the agency had developed with the intent of supporting a zero trust architecture. GAO compared Secret Service plans to OMB requirements and industry best practices.

GAO also reviewed configuration settings and interviewed agency officials about the milestones. GAO reviewed additional actions that the agency either had underway, or intended to take, to determine if the actions would meet OMB's requirements.

What GAO Recommends

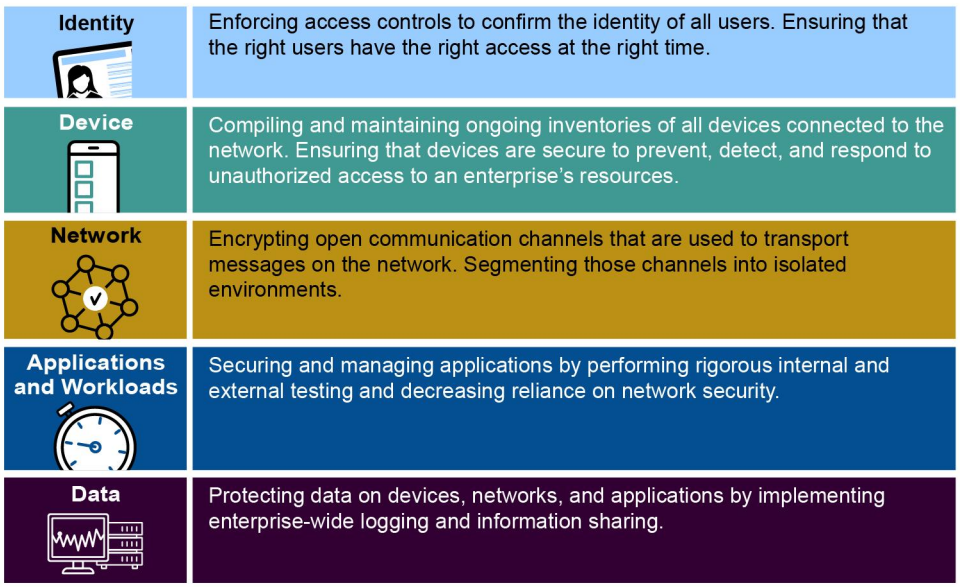
GAO is making two recommendations to the Secret Service, including to transition to a more advanced internet protocol for its public-facing systems and to update its zero trust architecture implementation plan. DHS, on behalf of Secret Service, concurred with the recommendations.

View GAO-23-105466. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

A zero trust architecture is a set of cybersecurity principles stating that organizations must verify everything that attempts to access their systems and services. These principles cover five pillars (see figure).

Cybersecurity and Infrastructure Security Agency Pillars of Zero Trust Architecture



Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency's *Zero Trust Maturity Model Version 1.0* (draft) and other relevant federal policies and guidance; images: lembergvector/stock.adobe.com. | GAO-23-105466

Text of Cybersecurity and Infrastructure Security Agency Pillars of Zero Trust Architecture

- Identity: Enforcing access controls to confirm the identity of all users. Ensuring that the right users have the right access at the right time.
- Device: 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.
- Network: 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 1.0 (draft) and other relevant federal policies and guidance; images: lembergvector/stock.adobe.com. | GAO-23-105466

The U.S. Secret Service developed an implementation plan for four milestones intended to support a zero trust architecture. The milestones are to (1) perform a self-assessment of the agency's IT environment against federal guidance, (2) implement cloud service offerings from a vendor, (3) achieve maturity in event logging, and (4) transition the agency's IT infrastructure to a more advanced internet protocol. Secret Service completed a self-assessment, and made progress in implementing cloud services and achieving maturity in event logging. In addition, the agency had a plan to implement a more advanced internet protocol, but had not met longstanding Office of Management and Budget (OMB) requirements for public-facing systems. By transitioning to this protocol, the agency can leverage additional security features.

Secret Service had additional efforts underway that could address actions specified in OMB's zero trust strategy issued in January 2022. However, because Secret Service developed its implementation plan before OMB issued the strategy, the plan's milestones do not cover all of OMB's required actions. Further, Secret Service has not updated its implementation plan to reflect these additional efforts. Doing so would provide agency management with a comprehensive and unified view of disparate activities associated with the zero trust architecture transition process.

Contents

Figures

Abbreviations

ABAC	attribute-based access control
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DNS	domain name system
EDR	endpoint detection and response
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure

IPv6	internet protocol version 6
ISP	internet service provider
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	personal identity verification
RBAC	role-based access control
VPN	virtual private network
ZTA	zero trust architecture

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

November 15, 2022

The Honorable Ron Johnson
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate
The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Michael McCaul
House of Representatives

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

Compounding these risks, federal systems and networks are often interconnected with other internal and external systems and networks, including the internet. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Since 1997, GAO has designated information security as a government-wide high-risk area—a designation that remains today.[1]

Having appropriate safeguards in place is particularly important for an agency such as the United States Secret Service (Secret Service), which relies heavily on the use of IT infrastructure and communications systems to accomplish its mission. Commonly known for protecting the President,

[1]See GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997); *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021). In 2003, we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.

the Secret Service, a component of the Department of Homeland Security (DHS), also plays a leading role in investigating and preventing a variety of financial and electronic crimes. For example, the Secret Service's criminal investigation activities encompass financial and electronic crimes, such as identity theft, counterfeiting, and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.

A May 2021 executive order marked a renewed commitment to, and prioritization of, federal cybersecurity modernization and strategy.[2] Among other policy mandates, the order requires that agencies adopt security best practices, including those associated with zero trust architectures (ZTA). ZTA is a set of cybersecurity principles that 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.

Transitioning to zero trust architectures will not be a quick or easy task for an enterprise as complex and technologically diverse as the federal government. While the concepts behind zero trust are not new, the implications of shifting away from perimeter-based security are new to most enterprises, including many federal agencies.[3] Further, agencies will have to continually evolve their zero trust environments moving forward in response to new technologies, vulnerabilities, and threats.

You asked us to review, among other things, cybersecurity at the U.S. Secret Service. Given the May 2021 executive order's emphasis on security best practices, our objective for this review was to evaluate Secret Service's implementation of a zero trust architecture. To do so, in November 2021 we requested the agency's ZTA implementation plan.[4] In response, the agency provided us with a plan that consisted of four milestones intended to substantially support a zero trust architecture, which involve:

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

[3]Perimeter-based security refers to conventional network security practices in which, once a user is inside of an organization's network, that user is considered trusted and is often given broad access to multiple resources.

[4]The scope of our review did not include any classified IT infrastructure.

1. performing a self-assessment of the agency IT environment against draft Cybersecurity and Infrastructure Security Agency (CISA) ZTA guidance,[5]
2. implementing cloud-based services provided by a vendor,
3. achieving a preliminary level of event logging maturity per Office of Management and Budget (OMB) guidance,[6] and
4. transitioning agency devices and systems to support internet protocol version 6 (IPv6).[7]

We reviewed activities associated with each of the four milestones. For the first milestone, we reviewed a self-assessment that the agency had completed using draft CISA guidance. In doing so, we identified Secret Service's determination of its maturity level for specific activities as either traditional, advanced, or optimal.

For the next milestone, we reviewed cloud-based services related to zero trust architecture.[8] Specifically, we reviewed cloud elements supported by a vendor that Secret Service chose to implement, and determined which elements would support the principles of ZTA. To do so, we reviewed agency planning documentation, and reviewed corroborating evidence as applicable, such as configuration settings.

For the third milestone, we reviewed and compared agency plans to reach maturity in event logging against OMB guidance. We also assessed corroborating documentation, as applicable, to describe the status of event logging at the agency for the third milestone.

To evaluate the fourth milestone, we reviewed the configuration of Secret Service's email and public-facing servers to determine the extent to which

[5]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model Version 1.0* (draft) (Washington, D.C.: June 2021). As of November 2022, the *Zero Trust Maturity Model* remains in draft format. CISA is an agency within the Department of Homeland Security.

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

[7]Internet protocol version 6 (IPv6) is the next generation of internet protocols, which are addressing mechanisms that define how and where information moves across interconnected networks. IP version 4 preceded IPv6.

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

the agency had enabled IPv6 in accordance with OMB requirements.[9] We also reviewed Secret Service plans and strategy for transitioning to IPv6.

We also reviewed documentation associated with the agency's overall planning processes. We compared the activities associated with the milestones to actions required in OMB's strategy.[10] In addition, we reviewed the status of efforts at the agency that were not included in the milestones, and reviewed corroborating documentation, as applicable. We compared activities to OMB's required actions to determine the extent to which additional efforts addressed the remaining required actions. Further, we evaluated the agency's implementation process for its ZTA plan and additional efforts against industry best practices.[11] In addition, we interviewed Secret Service Office of the Chief Information Officer (OCIO) officials about the status of the milestones and additional efforts.

We conducted this performance audit from October 2021 to November 2022 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.

Background

The zero trust security model assumes that a breach of IT systems is inevitable or has likely already occurred. Zero trust security is intended to continually limit user access to only the resources that users need, when they need them. As such, the zero trust model seeks to eliminate implicit trust in users or in devices connected to an agency's network. ZTA requires continuous verification of users or devices via real-time

[9]Office of Management and Budget, *Completing the Transition to Internet Protocol Version 6 (IPv6),* M-21-07 (Washington, D.C.: Nov. 19, 2020). Previous guidance included, specifically, *Transition to IPv6* (Washington, D.C.: Sept. 28, 2010).

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

[11]Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration® for Services* (CMMI-SVC), Version 1.3*,* CMU/SEI 2010 TR 034 (Pittsburgh, PA: November 2010).

information fed from multiple sources to determine access and other system responses.

ZTA embeds comprehensive security monitoring, granular risk-based access controls, and system security automation in a coordinated manner throughout all aspects of the infrastructure. This allows agency management to focus on protecting critical assets (e.g., data) in real time within a dynamic threat environment.

According to the National Institute of Standards and Technology (NIST), at a high level, zero trust architectures can be comprised of both core and functional components, which include, but are not limited to:[12]

- **Core components** that make and enforce decisions about whether or not to allow access to enterprise resources by users. They are comprised of:
  - ***Policy decision points*** that are responsible for the ultimate decision to grant access to a resource for a given subject, and for establishing or shutting down communication between a subject and a resource.[13] The policy decision point employs an algorithm, known as a trust algorithm, that is leveraged to ultimately grant or deny access to a resource.[14]
  - ***Policy enforcement points*** that enable, monitor, and eventually terminate connections between a subject and an enterprise resource.
- **Functional components** that are data sources that provide input and policy rules used by the policy decision point when making access decisions. Functional components can include:
  - ***Data security,*** which includes data access policies and rules that an enterprise develops to secure its information.

[12]National Institute of Standards and Technology, National Cybersecurity Center of Excellence, *Implementing a Zero Trust Architecture* (project description) (Rockville, MD: October 2020).

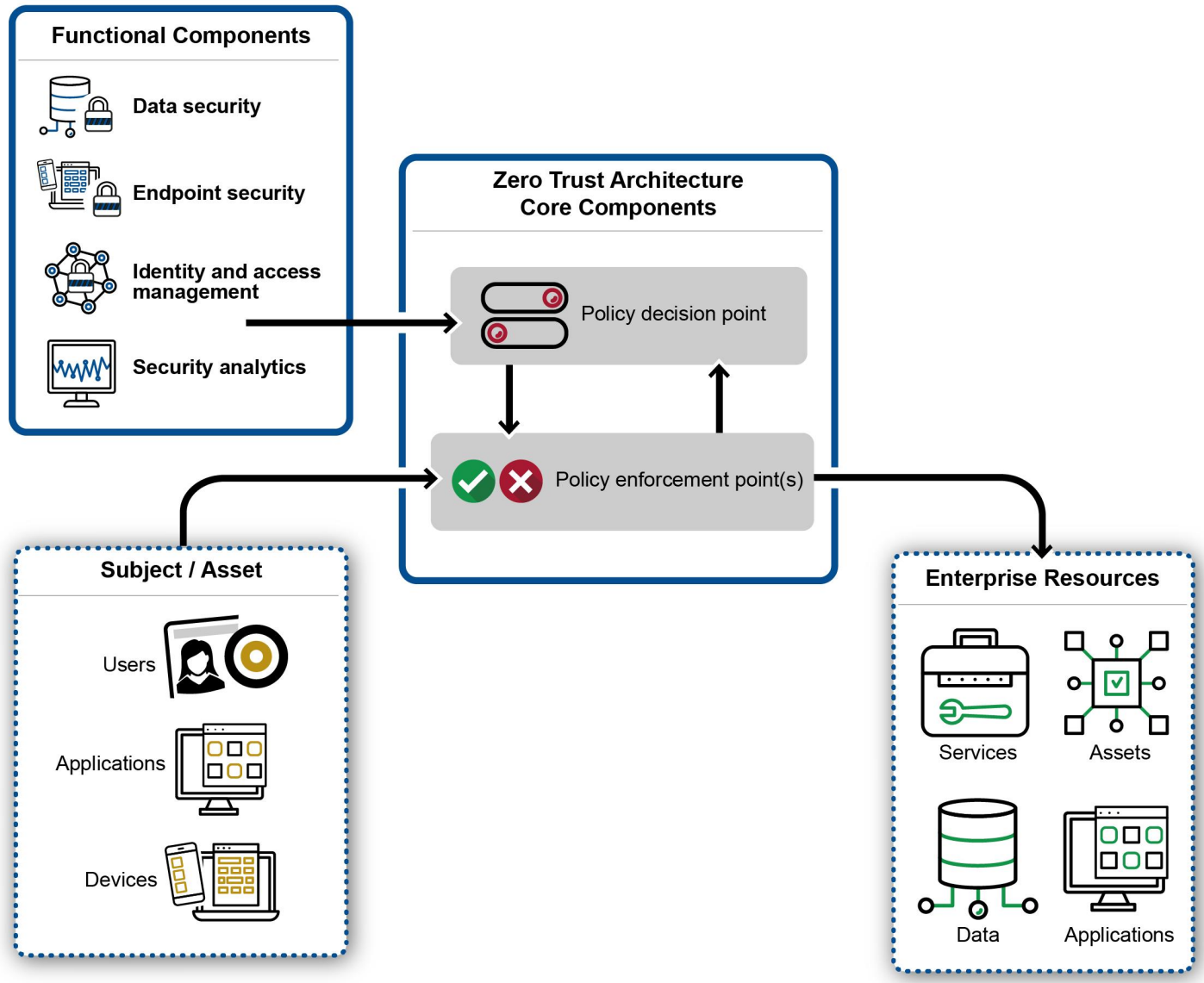
[13]A subject includes, for example, a user who is attempting to access an organization's resources, such as data or an application.

[14]According to the National Institute of Standards and Technology, the trust algorithm relies on observable information about subjects; subject attributes and roles; historical subject behavior patterns; threat intelligence; and other metadata sources; to determine whether or not to grant access to a resource. There are a variety of different ways to implement trust algorithms, including providing different weights to the factors relied on by the algorithm. Algorithms can be proprietary, or can be created by an entity for its specific purposes.

- ***Endpoint security,*** which encompasses the strategy, technology, and governance to protect endpoints (e.g., servers, desktops, phones, etc.) from threats and attacks.
- ***Identity and access management,*** which includes the strategy, technology, and governance for creating, storing, and managing enterprise user (i.e., subject) accounts.
- ***Security analytics,*** which encompass all the threat intelligence feeds and traffic/activity monitoring for an IT enterprise, and gathers security and behavior analytics about the current state of enterprise assets and continuously monitors those assets to actively respond to threats or malicious activity.

The core and functional components manage whether subjects or assets (e.g., users, applications, devices) have access to enterprise resources (e.g., services, assets, data, applications). Figure 1 shows a potential organization of the zero trust core and functional components, and the purposes the components serve in providing or denying user access to enterprise resources.

Figure 1: High-Level Zero Trust Architecture Developed by the National Institute of Standards and Technology



Source: GAO interpretation of National Institute of Standards and Technology zero trust architecture concept; image: lembergvector/stock.adobe.com. | GAO-23-105466

Text of Figure 1: High-Level Zero Trust Architecture Developed by the National Institute of Standards and Technology

- Functional Components
  - Data security
  - Endpoint security

    - Identity and access management
    - security analytics
- Subject / Asset
    - Users
    - Applications
    - Devices
- Enterprise Resources
    - Services
    - Assets
    - Data
    - Applications
- Zero Trust Architecture Core Components
    - Policy decision point (input from functional components)
    - Policy Enforcement point(s) (input from subjects and assets; policy decision points) (outputs to Enterprise Resources and feedback to policy decision point)

Source: GAO interpretation of National Institute of Standards and Technology zero trust architecture concept; image: lembergvector/stock.adobe.com. | GAO-23-105466Federal Guidance on Zero Trust Architectures

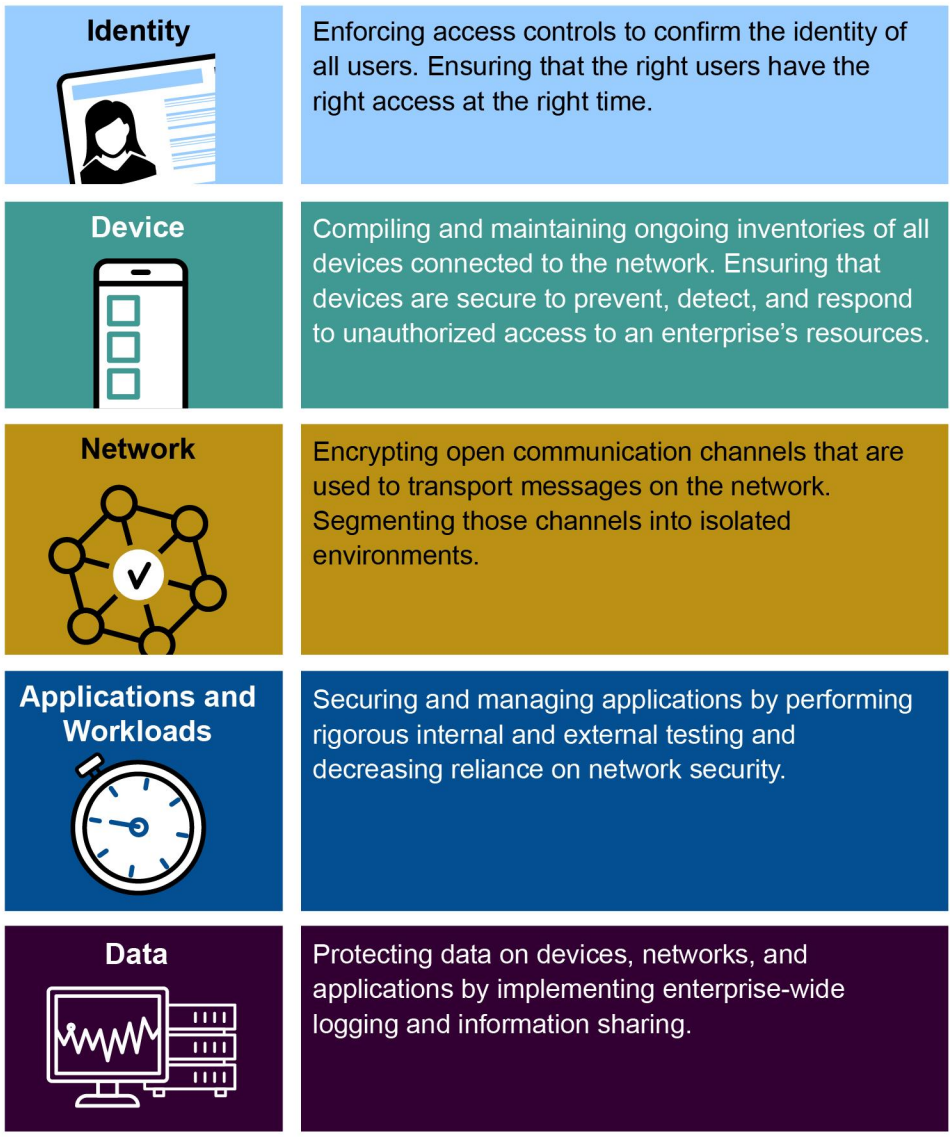
CISA, OMB, and NIST have developed guidance for federal agencies as they attempt to implement ZTA.

CISA: As previously noted, CISA created draft guidance in June 2021, the *Zero Trust Maturity Model 1.0,* which is intended to aid agencies in implementing ZTA.[15] The model is intended to support agencies in a rapidly evolving environment and technology landscape by focusing on modernization efforts related to zero trust. The CISA maturity model notes that it is one of many methods available to support the transition to zero trust.

CISA organized its *Zero Trust Maturity Model 1.0* across five pillars that support the foundation of zero trust: identity, device, network, applications, and data. Figure 2 describes the five pillars:

[15]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model Version 1.0* (June 2021, draft).

Figure 2: The Cybersecurity and Infrastructure Security Agency's Five Pillars of Zero Trust Architecture



Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency's *Zero Trust Maturity Model Version 1.0* (draft) and other relevant federal policies and guidance; images: lembergvector/stock.adobe.com. | GAO-23-105466

Text of Figure 2: The Cybersecurity and Infrastructure Security Agency's Five Pillars of Zero Trust Architecture

- Identity: Enforcing access controls to confirm the identity of all users. Ensuring that the right users have the right access at the right time.

- Device: 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.
- Network: 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 1.0 (draft) and other relevant federal policies and guidance; images: lembergvector/stock.adobe.com. | GAO-23-105466

The pillars are broken down into functions that more granularly describe capabilities associated with each pillar. Functions include, for example, authentication, compliance monitoring, network segmentation, access authorization, and inventory management. For each pillar, functions also include capabilities associated with visibility and analytics, automation and orchestration, and governance. In total, each pillar has six functions, except for applications and workloads, which has seven functions. Appendix I provides a complete list of the maturity model's functions. Further, each of the pillars is assigned three rating levels intended to define the maturity of an organization's transition to ZTA—traditional, advanced, and optimal.[16] The maturity ratings are intended to enable agencies to track the gradual migration to zero trust architectures. CISA notes that increasing levels of detail and complexity, such as automated security processes, allow for distributed interoperability. Cross-pillar coordination and minor advancements can be achieved in order to get an optimal rating over time.

[16]According to the CISA model, a **traditional** rating consists of no cross-pillar coordination, manual security configurations, limited risk assessments, static security policies, and minimal traffic encryption. It also consists of minimal workflow integration, manual incident response, simple inventory management, and limited visibility into compliance. An **advanced** rating consists of limited cross-pillar coordination, basic workflow integration, some centralized identity control, some automated incident response, and some centralized visibility into compliance. An **optimal** rating consists of cross-pillar coordination, full traffic encryption, continuous access authorization, fully automated threat protection with real-time machine learning analytics, and constant device security monitoring and validation.

OMB: In January 2022, 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.[17] The strategy outlines actions that agencies are to take by the end of fiscal year (FY) 2024 that are intended to form a starting point to implementing zero trust architecture.[18] The actions are organized using the *Zero Trust Maturity Model 1.0* (draft) and five pillars of ZTA developed by CISA in 2021.

In July 2022, OMB published guidance concerning agencies' FY 2024 budget requests which highlighted, among other things, expectations concerning zero trust architecture.[19] Specifically, the guidance states that agencies are to prioritize the achievement of the zero trust strategy's goals through inclusion in agency budget submissions.

NIST: NIST guidance provides 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.[20] It discusses an abstract definition of ZTA, general deployment models, and examples of cases in which ZTA could improve an enterprise's overall IT security posture. Further, NIST prepared a white paper to connect its risk management framework[21] with agencies' implementations of zero trust architectures.[22]

[17]OMB, M-22-09. This memorandum's requirements are aimed at department-level entities in the federal government. However, for the purposes of this report, we believe that in order to complete actions throughout a department, many of the actions will also have to be completed by component agencies, such as Secret Service. We use the term "agency" throughout this report to refer to department-level entities, as well as Secret Service.

[18]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.

[19]Office of Management and Budget, *Administration Cybersecurity Priorities for the FY 2024 Budget*, M-22-16 (Washington, D.C.: July 22, 2022).

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

[21]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, revision 2 (Gaithersburg, MD: December 2018).

[22]National Institute of Standards and Technology, *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators* (Gaithersburg, MD: May 6, 2022).

In addition to the guidance provided to all federal agencies, DHS developed its own ZTA implementation plan in March 2022, and submitted it to OMB. The department plans to continue to build on its implementation plan per OMB requirements. For example, it intends to use an integrated project team to include components, such as Secret Service, in its planning processes to incorporate zero trust architecture enterprise-wide.

Secret Service Is Progressing in Implementing a ZTA, but Its Plan Does Not Incorporate All Required Actions

Secret Service has made progress in implementing the four milestones associated with its ZTA implementation plan that it created as a result of the May 2021 executive order. Specifically, it performed a self-assessment of its operating environment against elements of CISA's maturity model, began implementing cloud services, and had plans to achieve maturity in event logging. Further, the agency had plans in place to transition to IPv6, but had not implemented longstanding OMB requirements to configure public-facing systems to this protocol.

Secret Service's four milestones do not cover all of the actions required in OMB's strategy, which was published subsequent to Secret Service developing its implementation plan. Nevertheless, the agency either had efforts underway, or reported that it intended to perform activities that could cover the remaining actions. However, these additional efforts are not reflected in the agency's ZTA implementation plan.

Secret Service Assessed Its IT Environment to Evaluate ZTA Maturity

As of February 2022, Secret Service had performed an assessment of its IT environment based on the functions that make up the five pillars of zero trust architecture according to CISA's maturity model. Table 1 provides a list of the ratings—traditional, advanced, or optimal—that the Secret Service OCIO assigned the agency's IT environment for the functions that support each pillar of zero trust architecture at the time of assessment.

Table 1: Secret Service IT Environment Self-Assessment Ratings Based on 31 Functions of the CISA Zero Trust Maturity Model

Pillar	Traditional[a]	Advanced[b]	Optimal[c]
Identity	0	6	0
Device	2	4	0
Network	2	3	1
Applications and Workloads	1	6	0
Data	1	5	0
Total	**6**	**24**	**1**

CISA = Cybersecurity and Infrastructure Security Agency

Source: GAO analysis of U.S. Secret Service self-assessment based on CISA *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

[a]A traditional rating consists of no cross-pillar coordination, manual security configurations, limited risk assessments, static security policies, and minimal traffic encryption. It also consists of minimal workflow integration, manual incident response, simple inventory management, and limited visibility into compliance.

[b]An advanced rating consists of limited cross-pillar coordination, basic workflow integration, some centralized identity control, some automated incident response, and some centralized visibility into compliance.

[c]An optimal rating consists of cross-pillar coordination, full traffic encryption, continuous access authorization, fully automated threat protection with real-time machine learning analytics, and constant device security monitoring and validation.

OCIO officials told us that they intended to use the self-assessment to strategize and plan to build their zero trust architecture. The officials added that the self-assessment would also enable them to identify gaps to inform future resource and logistics decisions.

Secret Service Plans to Further Implement Cloud Services from a Vendor

NIST highlights the adoption of cloud technologies in its zero trust architecture publication.[23] This publication emphasizes that resources, applications, and services that are primarily cloud-based or primarily used by remote workers are good candidates for a ZTA approach.

Secret Service has begun to, and plans to further implement a cloud service provider's offerings.[24] For example, the agency had integrated its cloud-based authentication service with on-premises authentication processes to synchronize and manage user accounts across its IT

[23]NIST Special Publication 800-207.

[24]Offerings consist of, for example, components and services available in the cloud instead of on premise.

environment. The agency also plans to deploy tools to leverage a cloud-based solution that should enable management of user and device identities using non-graphical user interfaces, such as scripts and command line tools. In addition, as of April 2022, Secret Service had plans in place to implement a component from its cloud services provider intended to support encryption of data at rest in the cloud.

Secret Service Has Plans to Achieve Maturity in Event Logging

In order to implement ZTA, agencies must have accurate, extensive, and timely event logging in place so that they can monitor, review, and analyze their assets in real time and forensically in the case of an event. Event logging is an essential component of security. It increases visibility into systems and networks in order to provide detection, investigation, and remediation of cyber threats of all types.

OMB memorandum M-21-31 states that information from logs on federal information systems is invaluable in the detection, investigation, and remediation of cyber threats. The memorandum outlines a maturity model that agencies are to follow in order to enhance their event logging, log retention, and log management activities. The maturity model consists of four levels, or tiers, as shown in table 2.

Table 2: Office of Management and Budget Memorandum M-21-31 Event Logging Tiers

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

Source: GAO analysis of information from Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,* M-21-31 (Washington, D.C.: Aug. 27, 2021). | GAO-23-105466

The levels are intended to help agencies prioritize efforts and resources in order to achieve compliance with implementation requirements by providing steps and guidance toward those goals. The levels are supported by technical logging requirements, which detail specific data that agencies must collect, including collection format and retention periods for different levels of criticality.

Secret Service set a goal to achieve the basic level of event logging maturity by August 2022 as one of four milestones that it intends to leverage in order to support a zero trust architecture. In support of achieving this milestone, the agency had additionally documented plans to implement the event logging requirements at each subsequent maturity level. The plans contained information specific to each of the levels and included, but were not limited to:

- **Tasks:** high-level item to be implemented based on event logging tier.
- **Descriptions:** detailed components to be implemented at a system level, including retention period requirements and additional data specific to Secret Service's implementation.
- **Creation dates, start dates, completion dates:** the date the task was added to the agency's plans, as well as dates implementation began and concluded.
- **Checklist items:** granular items that need to be implemented for each individual task.

As of August 2022, Secret Service had not yet achieved the basic level of event logging maturity according to its plans, although the agency had implemented a tool for centralized logging, monitoring, review, and analysis. Agency OCIO officials told us that implementation of OMB's specific event logging requirements was delayed due to administrative problems associated with a contract for a new tool that the agency planned to leverage to implement the maturity model requirements. The officials explained that, while the contract to implement the tool is in place, the agency cannot use the tool until it has completed administrative items associated with the contract.

Officials also stated that they expect the new tool to be in place no later than the end of FY 2022. The officials further stated that, once the tool is implemented, they intend to quickly implement the event logging tasks. OCIO officials stated that they believe the agency will use the current tool to identify gaps in the progress they have made in implementing the OMB logging requirements.

Secret Service Has Plans to Transition Devices and Services to Internet Protocol Version 6, But Has Made Limited Progress

An internet protocol (IP) provides the addressing mechanism that defines how and where information moves across interconnected networks, such

as the internet. Increased use of the internet has exhausted available IP version 4 (IPv4) address space, spurring the adoption of its successor protocol, IPv6. In addition to the benefit of eliminating the IPv4 address scarcity problem, IPv6 can allow for the use of enhanced security. As a result, IPv6 provides a receiver (e.g., a federal agency), with a greater assurance of a sender's identity.[25] By implementing IPv6, Secret Service can leverage enhanced flexibility and security features in its zero trust environment, including, for example, greater identity assurance and data protection.

OMB published requirements in November 2020 intended to update guidance on the federal government's operational deployment and use of IPv6.[26] It rescinded previous OMB guidance, including *Transition to IPv6* from 2010, but maintained two actions from the 2010 memorandum that it indicates are still relevant. In particular, the 2010 memorandum specified that agencies were to:

- upgrade public/external facing servers and services (e.g., web, email, domain name system (DNS), internet service provider (ISP) services, etc.) to operationally use IPv6 by the end of FY 2012, and
- upgrade internal client applications that communicate with public internet servers and supporting enterprise networks to operationally use IPv6 by the end of FY 2014.[27]

In addition, the 2020 memorandum requires that agencies transition to IPv6-enabled assets over a period of time between fiscal years 2023 and 2025.[28] Further, DHS developed guidance that, among other things, directs its components such as Secret Service to implement IPv6 in line with OMB requirements.

[25]GAO, *Internet Protocol Version 6: DOD Needs to Improve Transition Planning*, GAO-20-402 (Washington, D.C.: June 1, 2020).

[26]Office of Management and Budget, *Completing the Transition to Internet Protocol Version 6 (IPv6),* M-21-07 (Washington, D.C.: Nov. 19, 2020). Previous guidance included, specifically, *Transition to IPv6* (Washington, D.C.: Sept. 28, 2010).

[27]Operational use refers to direct support of IPv6 by systems and services, without the need for the use of IPv4 for communications.

[28]Agencies are to transition at least 20 percent of internet protocol (IP)-enabled assets to operate only in internet protocol version 6 (IPv6) by the end of fiscal year 2023, at least 50 percent of assets by the end of fiscal year 2024, and at least 80 percent by the end of fiscal year 2025.

Secret Service had plans for a transition to IPv6. For example, the agency OCIO developed a high-level strategy associated with the agency's IPv6 transition initiative. The May 2021 strategy outlines milestones and projected costs associated with transitioning up to 80 percent of Secret Service assets to IPv6, in line with OMB requirements.

However, as of August 2022, Secret Service had not begun the implementation process to support the transition to IPv6 for any of its assets or services. For example, Secret Service public email servers did not accept IPv6 email, and did not have IPv6 operationally enabled, although OMB required agencies to do so by the end of FY 2012. Specifically, the agency had not published IPv6 domain name server records for its public mail servers, but rather only IPv4 records.[29] As a result, Secret Service could not accept internet email via IPv6, forcing external IPv6-enabled email systems to resort to IPv4 connectivity to deliver email to Secret Service.

In addition, as of August 2022, Secret Service had not configured eight public-facing systems to operationally use IPv6. Because of this, the agency could not accept external IPv6 connections to the systems it lists as public-facing. This forced external IPv6-enabled clients to fall back to IPv4 connectivity to connect to the systems.

Secret Service OCIO officials told us in May 2022 that they did not have insight into any constraints that prevented the agency from upgrading public or external-facing servers and services to operationally use native IPv6 by the end of FY 2012.

The OCIO officials also explained that they had not been able to begin the transition due to funding constraints that were associated with a series of continuing resolutions passed during FY 2022.[30] The constraints prevented the agency from providing funds for the personnel and equipment required to transition assets to IPv6, according to OCIO officials. As of August 2022, OCIO officials told us that they had received funding and were in the process of obligating the funds for execution of their plan.

[29]A domain name system (DNS) is a protocol that translates domain names into IP addresses using DNS servers. Each DNS server maintains a database of domain names (hostnames) and their corresponding IP addresses.

[30]A continuing resolution is an appropriation act that provides budget authority for federal agencies, specific activities, or both to continue operating when Congress and the President have not completed action on the regular appropriation acts by the beginning of the fiscal year.

Until Secret Service fully transitions its assets to IPv6, and enables its services such as email to accept IPv6 communications, it will not be able to leverage the security features that IPv6 can provide. As such, the agency runs the risk that it will not build the end-to-end visibility that is possible with IPv6 into its systems and services as it continues to implement zero trust practices within its IT environment. Further, the agency will not be able to meet one of the four milestones that it intends to support its implementation of a zero trust architecture.

Secret Service Has Additional Efforts Underway to Address Subsequent OMB Requirements

Subsequent to Secret Service's development of the four milestones intended to substantially support a zero trust architecture, OMB published the federal zero trust strategy that includes 15 actions that agencies will have to take as they implement zero trust architectures. The strategy outlines actions that OMB expects agencies to take, in general, by the end of FY 2024.The actions are aligned with the five ZTA pillars of CISA's draft maturity model.

Secret Service has taken steps to address six of the 15 OMB required actions by including these actions within its 4-milestone plan (see Table 3 below). In addition to efforts associated with the milestones, the agency has efforts underway to address seven additional actions, and intends to address seven actions through additional efforts, as shown in Table 3.

Table 3: OMB Zero Trust Strategy Requirements Reflected in Secret Service's Zero Trust Architecture (ZTA) Milestones and Additional Efforts

			Efforts not included in Secret Service milestones	
ZTA pillar	**OMB required action**	**Efforts included in Secret Service milestones**	**Secret Service has additional efforts underway**	**Secret Service intends to take additional actions**
Identity	1. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.	X		
	2. Agencies must use strong multifactor authentication throughout their enterprise.	X		
	3. When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.[a]	X		

ZTA pillar	OMB required action	Efforts included in Secret Service milestones	Efforts not included in Secret Service milestones: Secret Service has additional efforts underway	Efforts not included in Secret Service milestones: Secret Service intends to take additional actions
Devices	1. Agencies must create reliable asset inventories through participation in the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation program.[b]		X	X
	2. Agencies must ensure their endpoint detection and response tools meet CISA's technical requirements and are deployed widely.[c]		X	X
Networks	1. Agencies must resolve domain name system (DNS) queries using encrypted DNS wherever it is technically supported.[d]			X
	2. Agencies must enforce hypertext transfer protocol secure[e] for all web and application program interface traffic in their environment. [f]		X	X
Applications and Workloads	1. Agencies must operate dedicated application security testing programs.		X	
	2. Agencies must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems.		X	
	3. Agencies must identify at least one internal-facing application and make it fully operational and accessible over the public internet.		X	X
	4. Agencies must provide any non-.gov hostnames they use to CISA and GSA.		X	X
	5. Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.			X
Data	1. Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.	X		
	2. Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.	X		
	3. Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB guidance on event logging maturity.	X		

OMB = Office of Management and Budget; GSA = General Services Administration

Source: GAO analysis of U.S. Secret Service milestones intended to support implementation of zero trust architecture against actions outlined in Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09. | GAO-23-105466

[a]A device-level signal can provide additional confidence during the user authentication process that a device is recognized by an organization and secured adequately.

[b]The Continuous Diagnostics and Mitigation program aims to help federal agencies achieve foundational awareness of their assets across the enterprise, and provides a suite of services intended to support improved monitoring and detection of assets.

[c]Endpoint detection and response tools are intended to support the proactive detection of cybersecurity incidents, as well as capabilities used when responding to those incidents.

[d]A DNS record is a database record used to map a uniform resource locator (or URL) to an internet protocol address. DNS records are stored in DNS servers and work to help users connect their websites to the outside world.

[e]Hypertext transfer protocol (HTTP) is a protocol for sending documents from one system to another on the internet; the more secure version is hypertext transfer protocol secure (HTTPS).

[f]An application program interface is a software interface that enables applications to communicate.

As shown in the above table, for seven of the remaining eight OMB requirements Secret Service has additional efforts underway that are currently not in its overall plan. For example:

- As of August 2022, Secret Service OCIO officials reported that they fully participate in the Continuous Diagnostics and Mitigation program, and meet or exceed DHS information security performance metrics.
- Secret Service had deployed a tool intended to provide endpoint detection and response (EDR) functionality across its IT environment.
- Secret Service officials told us that they were working within the scope of DHS's program for preloading .gov domains. DHS had also included the program in the zero trust planning documentation it provided to OMB in March 2022.
- Secret Service OCIO officials had documented the establishment of a software assurance governance committee, which is intended to provide an agency-wide approach for ensuring security testing, among other things, within the agency's IT environment.[31]
- Secret Service created a public vulnerability disclosure program that outlined policies intended to provide security researchers with clear guidelines for (1) conducting good faith vulnerability and attack vector discovery activities directed at their systems, and (2) submitting the discovered vulnerabilities to the agency.[32] The policies included an email address for reporting vulnerabilities, as well as guidelines for program participation, and expectations for participants and program results.

[31]The scope of the software assurance governance committee includes, among other things, ensuring that application and infrastructure architecture adequately meets all relevant security and compliance requirements, and sufficiently mitigates identified security threats.

[32]Secret Service made this program available on its public-facing website, https://www.secretservice.gov.

- Secret Service OCIO officials told us that, as of August 2022, they had selected a system to make fully operational and accessible over the public internet.
- Secret Service had begun to provide non-.gov hostnames used by their internet-accessible information systems to CISA through the Cyber Hygiene program.

Secret Service intends to take two actions, also not included in its current overall plan, that would address the remaining outstanding OMB requirements. Specifically:

- Agency OCIO officials told us that they intend to leverage CISA's Protective DNS Resolver Service to encrypt DNS queries. The officials added that the agency had not developed specific implementation steps for enabling encrypted DNS as of May 2022. The officials explained that they plan to implement CISA's solution once the solution is no longer in a beta-test status.
- The agency intends to deploy applications within immutable containers in order to approach immutable workloads required by OMB.[33] The officials added that they had begun the process of identifying candidate applications for this purpose, and had begun to research security monitoring solutions and continuous integration methods to integrate the applications into their environment.

Further, the Secret Service intends to take additional actions that will also contribute further to five of the OMB requirements for which the agency currently has efforts underway. Specifically:

- Secret Service OCIO officials reported that they intend to leverage the CDM program to fully manage their asset inventories. They described that leveraging will include delivery of cybersecurity tools, integration services, and dashboards to generate capability and visibility within the zero trust architecture.
- Agency OCIO officials reported that they intend to engage with DHS and CISA to support additional requirements associated with the agency's EDR functionality.
- Secret Service OCIO officials reported that they intend to leverage internal firewall traffic logs to identify current gaps in HTTPS and will develop plans to close those gaps.

[33]According to NIST, application container technologies, known as containers, provide a portable, reusable, and automatable way to package and run applications.

- Although Secret Service OCIO officials told us that they had selected a system to make fully operational and accessible over the public internet, they added that they did not yet have a time frame in mind for making the system accessible. However, the officials clarified that by fiscal year 2023, the agency will have a better understanding of the requirements for making the system accessible. They added that the agency may need to request additional funding to accomplish the task.
- Secret Service OCIO officials reported that they intend to work with DHS to ensure that non-.gov hostname information is provided to GSA in addition to CISA.

Appendix II provides more details on OMB's requirements and Secret Service's efforts and plans to address them. If implemented effectively, Secret Service's efforts could support implementation of OMB's requirements, which OMB considers to be a starting point for ZTA. Doing so should enhance the agency's ability to prevent unauthorized access to data and services and make access control enforcement as granular as possible. In addition, the actions should enhance the agency's ability to detect anomalous behavior, uniformly enforce security policies that limit access, as well as take action against anomalous behavior when needed.

Secret Service's ZTA Implementation Plan Does Not Address All OMB Requirements

Industry best practices suggest that entities should establish and maintain plans for performing processes intended to achieve specific goals.[34] The best practices further suggest that planning is one of the keys to effectively managing work, and includes developing and maintaining work plans.

As noted above, the four milestones in Secret Service's implementation plan address six of the 15 required actions. However, as of August 2022, Secret Service had not maintained its implementation plan by including its additional efforts in the plan. This condition existed because Secret Service developed its implementation plan before OMB disseminated its zero trust strategy in January 2022. If Secret Service does not keep its ZTA implementation plan up to date, management will likely not have a

[34]Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration® for Services* (CMMI-SVC), Version 1.3, CMU/SEI 2010 TR 034 (Pittsburgh, PA: November 2010).

coherent view of disparate activities associated with the transition process.

Conclusions

Adopting zero trust architectures will require vigilance in revamping existing IT environments to defend against ever-increasing threats. Although Secret Service has made progress, it has not yet addressed longstanding OMB requirements on implementing IPv6 for public-facing systems. By transitioning to this protocol, the agency can leverage additional security features.

Secret Service had also begun to undertake additional efforts not included in its implementation plan. These efforts, if implemented effectively, should help the agency address OMB's required actions. However, Secret Service did not update its ZTA implementation plan to reflect these additional efforts. Doing so would provide agency management with a comprehensive and unified view of disparate activities associated with the ZTA transition process.

Recommendations

We are making two recommendations to Secret Service:

The Director of the Secret Service should instruct the agency's chief information officer to implement outstanding Office of Management and Budget requirements for transitioning to IPv6, particularly in regard to upgrading its public-facing systems. (Recommendation 1)

The Director of the Secret Service should instruct the agency's chief information officer to update its ZTA implementation plan to include all efforts associated with the transition to ZTA. (Recommendation 2)

Agency Comments

We requested comments on a draft of this report from Secret Service. DHS responded on behalf of Secret Service and provided written comments, which are reprinted in appendix III. In its comments, the department concurred with both of our recommendations and provided Secret Service's estimated completion dates for implementing them. The department also provided technical comments, which we have incorporated into this report as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretary of DHS; the Director of the Secret Service; the DHS inspector general; and other interested congressional parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Jennifer R. Franks
Director
Information Technology and Cybersecurity

Appendix I: Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model Components

The following five tables list components associated with the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model 1.0 (draft) based on the five pillars that form the foundation of zero trust architecture.[1] The tables describe the functions associated with each pillar, as well as the traditional, advanced, and optimal ratings for each function.

Table 4: Functions Associated with the Identity Pillar of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model

Function	Traditional rating	Advanced rating	Optimal rating
Authentication	Agency authenticates identity using either passwords or multifactor authentication (MFA).	Agency authenticates identity using MFA.	Agency continuously validates identity, not just when access is initially granted.
Identity stores[a]	Agency only uses on-premises identity providers.	Agency federates some identity with cloud and on-premises systems.	Agency has global identity awareness across cloud and on-premises environments.
Risk assessment	Agency makes limited determinations for identity risk.	Agency determines identity risk based on simple analytics and static rules.	Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection.
Visibility and analytics capability	Agency segments user activity visibility with basic and static attributes.	Agency aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement.	Agency centralizes user visibility with high fidelity attributes and user and entity behavior analytics (UEBA).
Automation and orchestration capability	Agency manually administers and orchestrates (replicates) identity and credentials.	Agency uses basic automated orchestration to federate identity and permit administration across identity stores.	Agency fully orchestrates the identity life cycle dynamic user profiling, dynamic identity and group membership, just-in-time and just-enough access controls are implemented.

[1]Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model 1.0 (draft)* (Washington, D.C.: June 2021).

Function	Traditional rating	Advanced rating	Optimal rating
Governance capability	Agency manually audits identities and permissions after initial provisioning using static technical enforcement of credential policies (e.g., complexity, reuse, length, clipping, MFA, etc.).	Agency uses policy-based automated access revocation. There are no shared accounts.	Agency fully automates technical enforcement of policies. Agency updates policies to reflect new orchestration options.

Source: Cybersecurity and Infrastructure Security Agency *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

[a]Identity stores are a source for digital identities and their associated access rights to resources.

Table 5: Functions Associated with the Device Pillar of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model

Function	Traditional rating	Advanced rating	Optimal rating
Compliance monitoring	Agency has limited visibility into device compliance.	Agency employs compliance enforcement mechanisms for most devices.	Agency constantly monitors and validates device security posture.
Data access	Agency's access to data does not depend on visibility into the device that is being used to access the data.	Agency's access to data considers device posture on first-access.	Agency's access to data considers real-time risk analytics about devices.
Asset management	Agency has a simplified and manually tracked device inventory.	Agency uses automated methods to manage assets, identify vulnerabilities, and patch assets.	Agency integrates asset and vulnerability management across all agency environments, including cloud and remote.
Visibility and analytics capability	Agency's device management relies upon manual inspections of labels and periodic network discovery and reporting.	Agency reconciles device inventories against sanctioned lists with isolation of non-compliant components.	Agency continuously runs device posture assessments (e.g., using endpoint detection and response tools).
Automation and orchestration capability	Agency manually provisions devices with static capacity allocations.	Agency provisions devices using automated, repeatable methods with policy-driven capacity allocations and reactive scaling.	Agency's device capacity and deployment uses continuous integration and continuous deployment principles with dynamic scaling.
Governance capability	Agency manually defines and enforces device acquisition channels and establishes and implements inventory frequency policy. Device retirement requires extensive sanitation to remove residual access and data.	Agency devices natively support modern security functions in hardware. Agency minimizes the quantity of legacy equipment that is unable to perform desired security functions.	Agency devices permit data access and use without resident plain-text copies, reducing asset supply chain.

Source: Cybersecurity and Infrastructure Security Agency *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

Table 6: Functions Associated with the Network Pillar of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model

Function	Traditional rating	Advanced rating	Optimal rating
Network segmentation	Agency defines their network architecture using large perimeter/macro-segmentation.	Agency defines more of their network architecture by ingress/egress micro-perimeters with some internal micro-segmentation.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal micro-segmentation based around application workflows.
Threat protection	Agency bases threat protections primarily on known threats and static traffic filtering.	Agency includes basic analytics to proactively discover threats.	Agency integrates machine learning-based threat protection and filtering with context-based signals.
Encryption	Agency explicitly encrypts minimal internal or external traffic.	Agency encrypts all traffic to internal applications, as well as some external traffic.	Agency encrypts all traffic to internal and external locations, where possible.
Visibility and analytics capability	Agency provides visibility at perimeter with centralized aggregation and analysis.	Agency integrates analysis across multiple sensor types and positions with manual policy-driven alerts and triggers.	Agency integrates analysis across multiple sensor types and positions with automated alerts and triggers.
Automation and orchestration capability	Agency manually initiates and executes network and environment changes following change management workflows.	Agency uses automated workflows to manually initiate network and environment changes.	Agency network and environment configurations use infrastructure-as-code, with pervasive automation, following continuous integration and continuous deployment models.
Governance capability	Agency uses manual policies to identify sanctioned networks, devices, and services, with manual discovery and remediation of unauthorized entities.	Agency uses manual policies to identify sanctioned networks, devices, and services, with alerts and triggers and manual remediation for unauthorized entities.	Agency uses automated discovery of networks, devices, and services, with manual or dynamic authorization and automated remediation of unauthorized entities.

Source: Cybersecurity and Infrastructure Security Agency *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

Table 7: Functions Associated with the Applications and Workloads Pillar of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model

Function	Traditional rating	Advanced rating	Optimal rating
Access authorization	Agency's access to applications is primarily based on local authorization and static attributes.	Agency's access to applications relies on centralized authentication, authorization, monitoring, and attributes.	Agency continuously authorizes access to applications, considering real-time risk analytics.
Threat protection	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency has basic integration of threat protections into application workflows, primarily applying protections for known threats with some application-specific protections.	Agency strongly integrates threat protections into application workflows, with analytics to provide protections that understand and account for application behavior.

Function	Traditional rating	Advanced rating	Optimal rating
Accessibility	Some critical cloud applications are directly accessible to users over the internet, with all others available through a virtual private network (VPN).	All cloud applications and some on-premises applications are directly accessible to users over the internet, with all others available through a VPN.	All applications are directly accessible to users over the internet.
Application security	Agency performs application security testing prior to deployment, primarily through static and manual testing methods.	Agency integrates application security testing into the application development and deployment process, including the use of dynamic testing methods.	Agency integrates application security testing throughout the development and deployment process, with regular automated testing of deployed applications.
Visibility and analytics capability	Agency performs application health and security monitoring in isolation of external sensors and systems.	Agency performs application health and security monitoring in context with some external sensors and systems.	Agency performs continuous and dynamic application health and security monitoring with external sensors and systems.
Automation and orchestration capability	Agency establishes application hosting location and access at provisioning.	Applications can inform device and network components of changing state.	Applications adapt to ongoing environmental changes for security and performance optimization.
Governance capability	Agency has legacy policies and conducts manual enforcement for software development, software asset management, security tests and evaluations at technology insertion, and tracking software dependencies.	Agency has updated policies and centralized enforcement.	Agency has updated policies and dynamic enforcement.

Source: Cybersecurity and Infrastructure Security Agency *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

Table 8: Functions Associated with the Data Pillar of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model

Function	Traditional rating	Advanced rating	Optimal rating
Inventory management	Agency manually categorizes data and has poor data inventorying, leading to inconsistent categorization	Agency primarily inventories data manually with some automated tracking. Agency performs data categorization using a combination of manual and static analysis methods.	Agency continuously inventories data with robust tagging and tracking. Agency augments categorization with machine learning models.
Access determination	Agency governs access to data by using static access controls.	Agency governs access to data using least privilege controls that consider identity, device risk, and other attributes.	Agency's access to data is dynamic, supporting just-in-time and just-enough principles, and continual risk-based determinations.
Encryption	Agency primarily stores data in on-premises data stores and where they are unencrypted at rest.	Agency stores data in cloud or remote environments where they are encrypted at rest.	Agency encrypts all data at rest.

Function	Traditional rating	Advanced rating	Optimal rating
Visibility and analytics capability	Agency has limited data inventories that prevent useful visibility and analytics except possibly in specific circumstances.	Most of the agency's data are inventoried and can be accounted for since the last inventory update. Analytics are limited to plaintext data.	Agency's data are inventoried and can always be accounted for. Agency logs and analyzes all access events for suspicious behaviors. Agencies perform analytics on encrypted data.
Automation and orchestration capability	Agency lacks consistent categorization and labeling, which prevents automation and orchestration. Some data management tasks run automatically.	Agency runs scheduled audits that locate high-value data and analyze access controls. There is limited automatic orchestration to apply controls and ensure backups are in place.	Agency automatically enforces strict access controls for high-value data. All high-value data is backed up regardless of its storage location. Data inventories are automatically updated.
Governance capability	Agency largely enforces data protection and handling policies through administrative controls. Data categorization and data access authorizations are largely defined by distributed decision making.	Agency enforces data protections through mostly technical and some administrative controls. Data categorization and data access authorizations are defined with a method that better integrates diverse data sources.	Agency automatically always enforces data protections required by policy. Data categorization and data access authorizations are defined using a fully unified approach that integrates data, independent of source.

Source: Cybersecurity and Infrastructure Security Agency *Zero Trust Maturity Model 1.0* (draft). | GAO-23-105466

Appendix II: Description of Secret Service Efforts to Address the Office of Management and Budget's Zero Trust Architecture Requirements

This appendix is organized by the five pillars—identity, device, network, applications and workloads, data—in the Office of Management and Budget's (OMB) zero trust architecture strategy.[1] Within the pillars, OMB developed actions agencies are required to take by the end of fiscal year 2024.

Identity Pillar

- **Agencies must employ centralized identity management systems for users that can be integrated into applications and common platforms.**

  According to OMB's strategy, zero trust architectures require metadata about users to allow agencies to make risk-based decisions at the policy enforcement point.[2] Using centrally managed systems to provide enterprise identity and access management services reduces the burden on agency staff to manage individual accounts and credentials. It also improves agencies' knowledge of user activities, enabling better detection of anomalous behavior, among other things.

  Secret Service plans to implement components from its cloud services provider that should enable the agency to manage identity solutions across its enterprise, including for both on-premise and cloud-based systems and services. At the time of our review, the agency had integrated its cloud-based authentication service with on-premises authentication processes to synchronize and manage user accounts across its IT environment. Further, Secret Service Office of the Chief Information Officer (OCIO) officials told us they intended to engage

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

[2]A policy enforcement point is where policy decisions are carried out or enforced, such as authorization decisions.

with human resources staff at the agency to address any gaps that may exist in the integration.

In addition, the agency has plans to deploy tools to leverage a cloud-based solution that should enable management of user and device identities using non-graphical user interfaces, such as scripts and command line tools. This solution should help promote consistent and auditable identity practices enterprise-wide if effectively implemented.

- **Agencies must use strong multifactor authentication (MFA) throughout the enterprise.**

  OMB requires that agencies integrate and enforce MFA across applications involving authenticated access to systems by agency, staff, and partners.[3] The zero trust strategy requires that agencies enforce MFA in a number of ways. Secret Service intends to implement cloud-based services that should enable the agency to implement MFA. Specifically:

  - *Enforce MFA at the application layer instead of the network layer:*

    By implementing a centralized identity management solution as described above through its cloud services provider, Secret Service should be able to enforce MFA across its IT environment, and can do so at the application layer, instead of at the network layer. OCIO officials told us that they intend to leverage several cloud components to support this effort, which should also include the ability to enforce MFA to legacy applications.

  - *Provide phishing-resistant MFA to staff, contractors, and partners:*[4]

    Secret Service has implemented the use of personal identity verification (PIV) cards for use in authentication throughout its IT environment. The agency has integrated its PIV solution with its cloud-based authentication service to support phishing-resistant MFA across its enterprise to staff and contractors.

[3]OMB's requirements are generally not due until the end of fiscal year 2024. However, in this report, we say "OMB requires" in the present tense because agencies are currently working to fulfill the requirements.

[4]Phishing-resistant multifactor authentication (MFA) refers to processes that remove vulnerabilities that might undermine traditional MFA. For example, a short message service message used as MFA is highly vulnerable to being intercepted by a bad actor, whereas use of a personal identity verification card as MFA helps to remove such a vulnerability.

- *Agencies must provide public users with a phishing-resistant MFA option:*

  Secret Service OCIO officials told us that the agency does not have any public users, as it does not provide services for use by the general public. However, officials explained that the agency supports solutions for a few entities outside Secret Service, such as the banking and law enforcement industries, on its public-facing systems.

  As such, although the agency does not provide PIV cards for MFA to such users, the agency requires partner users to go through a third party identity-proofing process as part of the authentication process for particular partner services.[5] This process allows for a second factor of authentication for partner users.

- *Implement password policies that do not require use of special characters or regular rotation.*

  OMB encourages agencies to pursue greater use of "password-less" MFA as they modernize their authentication systems. The zero trust strategy requires that agencies remove password policies that require special characters and regular password rotation from all systems by January 26, 2023.

  As a result of its use of PIV as described above, as well as its authentication policy which prohibits the use of passwords for authentication to both non-privileged and privileged accounts, Secret Service had implemented this requirement. Further, the agency intends to implement additional cloud-based MFA services for some of its devices, such as through biometric solutions.

- **When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.**

  Many federal organizations rely on role-based access control (RBAC) to support user authorization. RBAC relies on static, predefined roles that are assigned to users and determine their permissions within an organization. However, according to OMB's strategy, zero trust architectures need to incorporate more granularly and dynamically defined permissions, such as those defined in attribute-based access control (ABAC). ABAC could consist of, for instance, a check based

[5]Identity proofing is the process of verifying that the claimed identity of a person matches their actual identity.

on a user's identity or the device with which the user is attempting access. For example, the check could look to see whether the device is known to the agency, and if its patches are up-to-date (known as device-level signals).

Secret Service intends to implement device-level signals as part of one of its cloud service provider's components. However, as of August 2022, the officials told us that they were working to resolve technical hurdles associated with the cloud component. Those hurdles will have to be overcome before they will be able to successfully implement the cloud component to support device-level signals alongside identity information during user authentication.

Device Pillar

- **Agencies must create reliable asset inventories through the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation (CDM) program.**[6]

  Secret Service OCIO officials reported that they intend to leverage the CDM program to fully manage their asset inventories. That leveraging will include delivery of cybersecurity tools, integration services, and dashboards to generate capability and visibility within the zero trust architecture. As of August 2022, OCIO officials added that they fully participate in the Department of Homeland Security (DHS) program, and meet or exceed DHS information security performance metrics.

- **Agencies must ensure that endpoint detection and response (EDR) tools meet CISA requirements and are deployed widely.**[7]

  In addition to requiring that agencies deploy EDR tools widely, OMB's strategy requires agencies to work with CISA to identify implementation gaps, coordinate the deployment of such tools, and establish information-sharing capabilities.

  Secret Service had deployed a tool intended to provide EDR functionality across its IT environment. But agency OCIO officials told us that they had not conducted a gap analysis of their capabilities in coordination with CISA, and had no plans for additional deployments between fiscal years 2023 to 2025. Further, the officials also told us

[6]The CDM program, operated by CISA, aims to help federal agencies achieve foundational awareness of their assets across the enterprise, and provides a suite of services intended to support improved monitoring and detection of assets.

[7]Endpoint detection and response tools are intended to support the proactive detection of cybersecurity incidents, as well as capabilities used when responding to those incidents.

that the agency did not have a plan to establish information sharing capabilities for data collected by the tools. However, OCIO officials told us that, from a practical standpoint, they intend to engage with DHS and CISA to accomplish these efforts.

Network Pillar

- **Agencies must resolve domain name system (DNS) queries using encrypted DNS wherever it is technically supported.**

  Although agency OCIO officials told us that they intend to leverage CISA's Protective DNS Resolver Service to encrypt DNS queries, the officials added that the agency had not developed specific implementation steps for enabling encrypted DNS as of May 2022. The officials explained that they plan to implement CISA's solution once the solution is no longer in a beta-test status.

- **Agencies must enforce hypertext transfer protocol secure (HTTPS) for all web and application program interface traffic in their environment.**

  Agency OCIO officials told us that Secret Service configuration standards require HTTPS rather than HTTP where technically possible. As such, they explained that they believed most internal systems/applications are already meeting this requirement. However, the officials added that the agency intends to leverage internal firewall traffic logs to identify current gaps and will then develop plans to close those gaps.

  In addition to enforcing HTTPS across the IT environment, OMB also expects agencies to work with CISA to preload their .gov domains into web browsers as only accessible over HTTPS.[8] Secret Service officials told us that they were working within the scope of DHS's program for preloading .gov domains. DHS had also included the program in the zero trust planning documentation it provided to OMB in March 2022. DHS indicated that components, such as Secret

[8]The .gov domain exists so that online services of bona fide U.S.-based government organizations are easy to identify on the internet. Because of this, CISA assumed responsibility for managing the .gov domain in 2021. Preloading refers to a process the modern web browsers can use to automatically load websites as hypertext transfer protocol secure (HTTPS). However, not all .gov websites are covered by this process because, for example, some may be older than May 15, 2017, which is the cutoff date for this process. The DotGov program exists to, among other things, enable agencies to support the preloading of websites that otherwise would not have been automatically preloaded in HTTPS.

Service, would continue to work with the program to preload their .gov domains to enable HTTPS capabilities.

Applications and Workloads Pillar

- **Agencies must operate dedicated application security testing programs.**

  OMB's strategy emphasizes that agencies will need to go beyond implementing and documenting security controls to enable their applications to withstand sophisticated probing and attack. As such, OMB requires agencies to analyze their software and its deployed functionality with a comprehensive and rigorous approach. Secret Service OCIO officials had documented the establishment of a software assurance governance committee at the agency, which is intended to provide an agency-wide approach for ensuring security testing, among other things, within the agency's IT environment.[9]

- **Agencies must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems.**

  In addition to robust internal testing programs, OMB's zero trust strategy emphasizes that agencies scrutinize their applications through external partners and independent perspectives to evaluate real-world security of agency applications, and include a process for coordinated disclosure of vulnerabilities by the general public.

  Secret Service created a public vulnerability disclosure program that outlined policies intended to provide security researchers with clear guidelines for (1) conducting good faith vulnerability and attack vector discovery activities directed at their systems, and (2) submitting the discovered vulnerabilities to the agency.[10] The policies included an email address for reporting vulnerabilities, as well as guidelines for program participation, and expectations for participants and program results. As of August 2022, the agency had not received any vulnerability reports from external sources through the program, but

[9]The scope of the software assurance governance committee includes, among other things, ensuring that application and infrastructure architecture adequately meets all relevant security and compliance requirements, and sufficiently mitigates identified security threats.

[10]Secret Service made this program available on its public-facing website, https://www.secretservice.gov.

indicated that it would expand the scope of the program as necessary as the agency adds additional systems.

- **Agencies must identify at least one internal-facing *Federal Information Security Modernization Act of 2014* (FISMA) Moderate application and make it fully operational and accessible over the public internet.**[11]

  According to OMB's strategy, making applications internet-accessible in a safe manner without the use of, for example, virtual private network infrastructure, is and will continue to be a major challenge for federal agencies.[12] As such, OMB seeks to take an incremental approach. To enable agencies to identify early obstacles in doing so, each agency must select at least one FISMA Moderate system that requires authentication and is not currently internet-accessible, and within one year make it accessible from the internet.

  Secret Service OCIO officials told us that, as of August 2022, they had selected a system to make fully operational and accessible over the public internet. However, the officials added that they did not yet have a time frame in mind for making the system accessible.

- **Agencies must provide any non-.gov hostnames they use to CISA and the General Services Administration (GSA)**

  According to OMB's strategy, to effectively implement a zero trust architecture, an organization must have a complete understanding of its internet-accessible assets, so that it may apply security policies consistently and fully define and accommodate user workflows. In practice, it can be very challenging for large, decentralized organizations to track every asset reliably. For agencies to maintain a complete understanding of what internet-accessible attack surface they have, they must rely not only on their internal records, but also on external scans of their infrastructure from the internet.

[11]Pursuant to the *Federal Information Security Management Act of 2002,* Pub. L. No. 107-347, title III, § 302(a), 116 Stat. 2946, 2957 (2002), the term federal information system refers to an information system used or operated by an executive agency, or by a contractor or organization on behalf of an agency. According to the National Institute of Standards and Technology, a system at the Moderate level is a system for which compromise would result in a serious adverse impact on organizational operations or individuals.

[12]OMB, M-22-09.

According to the strategy, CISA will provide data about agencies' internet-accessible assets obtained through public and private sources. As such, OMB required that agencies begin to provide CISA and GSA with any non-.gov hostnames used by their internet-accessible information systems. Secret Service had begun to provide information of this type to CISA through the Cyber Hygiene program, and intends to work with DHS to ensure that this information is also provided to GSA.[13]

- **Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.**

  OMB suggests that agency code or infrastructure should be deployed to a cloud environment in a way that technically restricts manual modification, and is immutable (i.e., resistant to change). Such deployments support zero trust goals by allowing improved least privilege architectures.

  OCIO officials reported that they intend to deploy applications within immutable containers in order to approach immutable workloads required by OMB.[14] The officials added that they had begun the process of identifying candidate applications for this purpose, and had begun to research security monitoring solutions and continuous integration methods to integrate the applications into their environment.

Data Pillar

- **Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.**

  According to OMB's strategy, in order to support their systems and cloud infrastructure during security events, agencies will find that automation of security monitoring and enforcement to be a practical necessity. Making automation work in a large enterprise will require careful tuning, iteration, and sensitivity to business needs. As such, OMB requires that agencies strive to employ heuristics rooted in machine learning to categorize the data they gather, and to deploy

[13]The CISA Cyber Hygiene program offers several scanning and testing services to help organizations reduce their exposure to threats by taking proactive approaches to mitigating attack vectors.

[14]According to NIST, application container technologies, known as containers, provide a portable, reusable, and automatable way to package and run applications.

processes that offer early warning or detection of anomalous behavior in as close to real time as possible.

Secret Service OCIO officials told us that the agency's Security Management Division and Cyber Security Program had discussed document marking in the context of sensitivity labels based on government-recognized data categories. They stated that, as of August 2022, they had begun to pilot sensitivity labels.

- **Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.**

  According to OMB's strategy, when agencies encrypt data at rest in the cloud, they must create a trustworthy audit log that documents attempts to access the data. Secret Service had plans in place to implement a component from its cloud services provider intended to encrypt data at rest in the cloud. The component also creates audit logs that the agency can leverage to review access to the encrypted data.

- **Agencies must work with CISA to implement comprehensive logging and information sharing capabilities, as described in OMB memorandum M-21-31.**[15]

  As of August 2022, Secret Service had not yet achieved the basic level of event logging maturity according to its plans, although the agency had implemented a tool for centralized logging, monitoring, review, and analysis. Agency OCIO officials told us that implementation of OMB's specific event logging requirements was delayed due to administrative problems associated with a contract for a new tool that the agency planned to leverage to implement the maturity model requirements. The officials explained that, while the contract to implement the tool is in place, the agency cannot use the tool until it has completed administrative items associated with the contract.

  Officials also stated that they expect the new tool to be in place no later than the end of fiscal year 2022. The officials further stated that, once the tool is implemented, they intend to quickly implement the event logging tasks. OCIO officials stated that they believe the agency

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

will use the current tool to identify gaps in the progress they have made in implementing the OMB logging requirements.

Appendix III: Comments from the Department of Homeland Security

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

Homeland Security

October 27, 2022

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

Re: Management Response to Draft Report GAO-23-105466, "CYBERSECURITY: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains"

Dear Ms. Franks:

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

DHS leadership is pleased to note GAO's recognition of the Secret Service's efforts to:

- Implement milestones intended to support a Zero Trust Architecture (ZTA), which were originally created in response to Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," dated May 12, 2021;[1] and
- Complete or initiate additional efforts to address additional Office of Management and Budget (OMB) and other requirements published subsequent to the development of Secret Service's implementation plan (e.g., OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," dated January 26, 2022,[2] and the Department of Homeland Security's "Zero Trust Implementation Strategy," dated March 2022, (ZTA Implementation Strategy)).

The Secret Service remains committed to an enterprise approach to implementing cost-effective solutions that meet or exceed federal cybersecurity standards, while maximizing the organizational capacity of its workforce.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

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

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

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2022.10.27 09:38:44 -04'00'

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

Enclosure

2

Enclosure: Management Response to Recommendations Contained in GAO-23-105466

GAO recommended that Director of the U.S. Secret Service instruct the agency's Chief Information Officer to:

Recommendation 1: Implement outstanding Office of Management and Budget requirements for transitioning to IPv6 [internet protocol version 6], particularly in regard to upgrading its public-facing systems.

Response: Concur. The Secret Service's Office of the Chief Information Officer (OCIO) will continue identifying requirements for transition to IPv6, pursuant to OMB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," dated November 19, 2020,[3] and the DHS ZTA Implementation Strategy, to include implementation milestones as documented in OMB M-21-07. This effort will include:

- Ensuring at least 20 percent of Internet Protocol (IP)-enabled assets on Federal networks are operating in IPv6-only environments by the end of fiscal year (FY) 2023;
- Ensuring at least 50 percent of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024;
- Ensuring at least 80 percent of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025; and
- Identifying and justifying Federal information systems that cannot be converted to use IPv6 and developing a schedule for replacing or retiring these systems by the end of FY 2025.

Overall Estimated Completion Date (ECD): September 30, 2025.

Recommendation 2: Update its ZTA implementation plan to include all efforts associated with the transition to ZTA.

Response: Concur. The Secret Service's OCIO will review its internal ZTA implementation plan and take action, as appropriate, to ensure that it incorporates guidance from the DHS ZTA Implementation Strategy and OMB guidance associated with the transition to ZTA. ECD: December 29, 2022.

[3] https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

3

Text of Appendix III: Comments from the Department of Homeland Security

October 27, 2022

Jennifer R. Franks

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105466, "CYBERSECURITY: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains"

Dear Ms. Franks:

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

DHS leadership is pleased to note GAO's recognition of the Secret Service's efforts to:

- Implement milestones intended to support a Zero Trust Architecture (ZTA), which were originally created in response to Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," dated May 12, 2021;[1] and
- Complete or initiate additional efforts to address additional Office of Management and Budget (0MB) and other requirements published subsequent to the development of Secret Service's implementation plan (e.g., 0MB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," dated January 26, 2022,[2] and the Department of Homeland

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

[2] https://www.whitehouse.gov/wp-content/uploads/2022/0 l/M-22-09.pdf

Security's "Zero Trust Implementation Strategy," dated March 2022, (ZTA Implementation Strategy)).

The Secret Service remains committed to an enterprise approach to implementing cost- effective solutions that meet or exceed federal cybersecurity standards, while maximizing the organizational capacity of its workforce.

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

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

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-23-105466

GAO recommended that Director of the U.S. Secret Service instruct the agency's Chief Information Officer to:

Recommendation 1: Implement outstanding Office of Management and Budget requirements for transitioning to 1Pv6 [internet protocol version 6], particularly in regard to upgrading its public-facing systems.

Response: Concur. The Secret Service's Office of the Chief Information Officer (OCIO) will continue identifying requirements for transition to 1Pv6, pursuant to 0MB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (1Pv6)," dated November 19, 2020,[3] and the DHS ZTA Implementation

[3] https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

Strategy, to include implementation milestones as documented in 0MB M-21-07. This effort will include:

- Ensuring at least 20 percent of Internet Protocol (IP)-enabled assets on Federal networks are operating in 1Pv6-only environments by the end of fiscal year (FY) 2023;
- Ensuring at least 50 percent of IP-enabled assets on Federal networks are operating in 1Pv6-only environments by the end of FY 2024;
- Ensuring at least 80 percent of IP-enabled assets on Federal networks are operating in 1Pv6-only environments by the end of FY 2025; and
- Identifying and justifying Federal information systems that cannot be converted to use 1Pv6 and developing a schedule for replacing or retiring these systems by the end of FY 2025.

Overall Estimated Completion Date (ECD): September 30, 2025.

Recommendation 2: Update its ZTA implementation plan to include all efforts associated with the transition to ZTA.

Response: Concur. The Secret Service's OCIO will review its internal ZTA implementation plan and take action, as appropriate, to ensure that it incorporates guidance from the DHS ZTA Implementation Strategy and 0MB guidance associated with the transition to ZTA. ECD: December 29, 2022.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director), West Coile (Assistant Director), Kevin Smith (Analyst-in-Charge), Chris Businsky, Ryan Fetrow, Chaz Hubbard, Sailaja Ledalla, Ashley Paw, and Priscilla Smith made key contributions to this report. Ahsan Nasar and Adam Vodraska also provided valuable assistance.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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