

NASA

Office of Inspector General

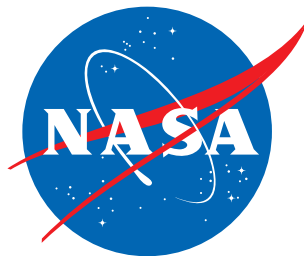


Audit of NASA's Zero Trust Architecture



March 27, 2025

IG-25-004



Office of Inspector General

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit <https://oig.nasa.gov/hotline.html>. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas or request future audits, contact the Assistant Inspector General for Audits at <https://oig.nasa.gov/oig-personnel/>.

RESULTS IN BRIEF

Audit of NASA's Zero Trust Architecture



March 27, 2025

IG-25-004 (A-24-08-00-MSD)

WHY WE PERFORMED THIS AUDIT

Zero trust architecture (ZTA) is a cybersecurity framework focused on “never trust, always verify.” Where traditional cybersecurity models enforce stringent defenses at a system’s perimeter but are more relaxed internally, zero trust consistently scrutinizes and constantly verifies every access request to a system. As required by the Office of Management and Budget, agencies, including NASA, are working to meet zero trust federal mandates. However, there is no single tool NASA can deploy to instantly implement ZTA as different system architectures are necessary for unique environments. Zero trust applied to a commercial, general-purpose Agency-wide information technology (IT) application, like email, is different than implementing zero trust for NASA-specific legacy systems in operation for decades. Modern techniques for cybersecurity, including ZTA, may be too risky for missions using old legacy technology, and NASA will have to determine whether ZTA capabilities can be employed on legacy systems. The challenge is delivering an Agency-wide ZTA that addresses cybersecurity vulnerabilities while protecting modern IT, such as systems and networks that process data; operational technology (OT), such as temperature sensors that control and monitor industrial equipment; and existing legacy systems and networks.

NASA’s IT architecture is divided into three distinct environments—(1) corporate, (2) mission, and (3) Jet Propulsion Laboratory (JPL)—and the Agency is using a staged approach to implement ZTA in phases. Currently, NASA’s ZTA efforts are focused solely on corporate systems with implementation of mission and JPL systems intended to follow in subsequent years. Corporate systems are managed by the Office of the Chief Information Officer (OCIO), which has overarching responsibility for NASA’s IT infrastructure and the ZTA initiative. Mission and JPL systems (collectively known as non-corporate systems) are managed independently. Mission directorates, centers, and headquarters offices are treated as separate “organizations,” each operating within their own boundaries including independently managing their own IT in areas such as budget, staff, contracts, and IT hardware and software.

In this audit, we assessed NASA’s progress and challenges in implementing ZTA with a focus on (1) policy, (2) legacy systems, and (3) cybersecurity. To complete this work, we reviewed federal and NASA policies, regulations, guidance, frameworks, and best practices. We interviewed OCIO officials responsible for ZTA implementation and stakeholders from NASA’s mission directorates. We determined whether legacy systems were identified and assessed the systems’ operational complexities and cybersecurity challenges. We also evaluated the OCIO’s engagement and collaboration with stakeholders to identify shortcomings that could affect ZTA implementation.

WHAT WE FOUND

NASA has made progress implementing ZTA within its corporate environment by appointing a zero trust strategy implementation lead, submitting its implementation plan to the Office of Management and Budget, and completing ZTA security actions. However, ZTA implementation for mission and JPL systems has not yet started. By focusing on the corporate environment and delaying mission and JPL systems, we found NASA’s ZTA strategy lacks an Agency-wide focus. NASA is missing an opportunity to address enterprise-wide issues such as organizational boundaries, integration hurdles, and operational complexities that will impact ZTA adoption within the non-corporate environment. Specifically, a lack of effective engagement between the OCIO and mission directorates is hindering implementation. This is largely due to the OCIO and mission directorates operating within their organizational boundaries and not consistently

collaborating or communicating, particularly during the implementation of new Agency-wide initiatives. Limited IT representation from mission directorates and centers on OCIO decision-making boards and a lack of clear lines of authority on IT matters within mission directorates further complicate the issue.

Integration hurdles also impact ZTA implementation. NASA operates under a diverse and complex federated model with subordinate organizations, such as mission directorates, retaining decision authority and budgets, while the OCIO provides Agency-wide coordination of IT efforts like ZTA. As a result, unique interoperability and other issues mission system owners face to secure IT assets are often unclear to the OCIO. Mission directorate officials told us had they been included in the early stages of ZTA implementation, they could have provided projects and mission systems to the OCIO to use as pathfinders, offering valuable insights to identify and resolve ZTA integration conflicts within mission-specific environments. By relegating mission and JPL environments to later ZTA phases, an opportunity was missed to identify and evaluate use cases—descriptions of how a user interacts with a system—prior to broader ZTA implementation.

External NASA stakeholders also complicate ZTA implementation as they may not have access to ZTA authentication methods like smartcards. In addition, most mission directorates use their own tools and computer security processes for identity and access management and authentication. NASA also lacks a centralized process to identify legacy IT and OT systems and does not maintain an inventory of the systems. Decisions to remain status quo or upgrade a legacy system are further complicated by operational, technical, and financial constraints. Without an Agency-wide program to identify, prioritize, and execute the updating, replacing, or retiring of legacy systems, migrating to ZTA will be delayed.

Finally, using a staged approach for ZTA implementation does not consider the unique IT and OT operational complexities specific to the mission directorates and JPL. Mission directorate officials are concerned about the OCIO's limited knowledge of the unique systems that make up NASA's complex mission environment and the impact that will have on ZTA implementation. NASA's engineering and scientific research communities use a "test like you fly" approach—an assessment and testing process pre-launch that reflects the planned mission—to ensure mission success and a solution that is technically safe, sound, and meets the objective prior to launching a mission. In our view, this approach should apply to the acquisition and implementation of new or upgraded IT and OT systems, as well as any changes that can impact these systems. Ultimately, the robustness of zero trust hinges on the ability to maintain a strong focus and collaborate on the implementation of ZTA across both corporate and non-corporate IT and OT systems.

WHAT WE RECOMMENDED

To expand NASA's ZTA adoption and address organizational boundaries, integration hurdles, and operational complexities, we recommended the Associate Administrator and Chief Information Officer: (1) collaborate with mission directorate officials to update NASA's ZTA implementation plan to include all efforts associated with the transition to ZTA within the non-corporate environment; (2) develop a centralized process to track legacy systems that details deficiencies along with operational, technical, and financial constraints to determine a best course of action for remediation; (3) embed OCIO subject matter experts within the mission directorates to provide Agency-focused advocacy and expertise to analyze mission system cybersecurity compatibility and operational complexities; and (4) engage mission directorates as ZTA pathfinders to identify and evaluate early adoption use-case candidates, employ a "test like you fly" approach, and provide insight to potential issues.

We provided a draft of this report to NASA management who concurred or partially concurred with our recommendations and described planned actions to address them. We consider management's comments responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

For more information on the NASA Office of Inspector General and to view this and other reports visit <https://oig.nasa.gov/>.

TABLE OF CONTENTS

Introduction	1
Background	2
NASA’s Shift to ZTA Is Progressing but Lacks an Agency-Wide Focus	11
Organizational Boundaries Limit Collaboration	11
Integration Hurdles Hinder ZTA Initiatives	13
Delaying Mission Directorate and JPL ZTA Implementation Obscures Operational Complexities and Erodes Progress.....	16
Conclusion	19
Recommendations, Management’s Response, and Our Evaluation	20
Appendix A: Scope and Methodology	21
Appendix B: NASA’s Zero Trust Implementation Status	23
Appendix C: Management’s Comments	26
Appendix D: Report Distribution	29

Acronyms

CIP	Cyber Improvement Portfolio
CISA	Cybersecurity and Infrastructure Security Agency
IT	information technology
JPL	Jet Propulsion Laboratory
MFA	multi-factor authentication
NASCOM	NASA Communications Network
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OT	operational technology
SCaN	Space Communications and Navigation
ZTA	zero trust architecture

INTRODUCTION

Zero trust architecture (ZTA)—a cybersecurity framework focusing on “never trust, always verify”—has evolved from a buzzword to dominating cybersecurity discussions across the federal government and private industry alike.¹ Unlike traditional cybersecurity models that enforce stringent defenses at a system’s perimeter, or boundary, but are more relaxed internally, zero trust treats every access request to a system with consistent scrutiny, regardless of its origin.² As ZTA is focused on relentless verification, organizations must constantly verify user and device privileges. In the government, implementing zero trust standards is a top priority as required by the Office of Management and Budget (OMB), especially with specific zero trust cybersecurity goals such as centralized identity management and asset inventories.³



Although agencies are working to meet various zero trust federal mandates and milestones, reaching higher levels of zero trust maturity across five key pillars—identity, devices, networks, applications and workloads, and data—is challenging.⁴ Failure to modernize technology devices, resource constraints, integration hurdles, and operational complexities often hinder progress in implementing ZTA and addressing long-standing cybersecurity vulnerabilities. Every agency faces unique challenges and considerations as part of its zero trust strategy, and NASA is no exception. Given its high-profile mission and broad connectivity with the public, educational institutions, and outside research facilities, NASA presents cyber criminals a larger potential target than most government agencies.

There is no single tool that NASA can deploy to instantly implement ZTA across all systems; different system architectures are necessary for different environments. Zero trust applied to a commercial, general purpose enterprise-wide (i.e., Agency-wide) information technology (IT) application, such as email or time cards, is different than implementing zero trust for a legacy system that has been operating for decades.⁵ For example, the architecture for data transmissions from the nearly 50-year-old Voyager 1 spacecraft—more than 15 billion miles from Earth—requires unique considerations.⁶ Voyager is an example of legacy technology so old that modern techniques for cybersecurity, including

¹ The zero trust framework describes a strict approach to cybersecurity in which every individual or device that attempts to access the network must be identified and authorized.

² A perimeter is a physical or logical boundary that is defined for a system within which a particular security policy or security architecture is applied.

³ OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022).

⁴ Pillars are complementary cybersecurity themes that cross functions within the ZTA model. Many capabilities depend on or align with capabilities in other pillars.

⁵ Outdated systems and components resulting from the neglect or delay of modernizing technology is known as legacy infrastructure.

⁶ Launched in 1977, Voyager 1 completed close flybys of Jupiter and Saturn and reached the interstellar boundary—the space between stars—in 2012. Now the mission is measuring magnetic fields, particles, and plasma waves in interstellar space.

implementing the zero trust framework, are likely too risky to that mission because of the spacecraft's age and location in interstellar space. Instead, NASA will have to determine whether select ZTA capabilities can be employed on legacy systems to mature the system's zero trust posture. The challenge is delivering an Agency-wide ZTA that protects modern IT, such as systems and networks that process data; operational technology (OT), such as temperature sensors that control and monitor industrial equipment; and existing legacy systems and networks.⁷

In this audit, we assessed NASA's progress and challenges in implementing ZTA, with a focus on (1) policy, (2) legacy systems, and (3) cybersecurity. See Appendix A for details of the audit's scope and methodology.

Background

Increasingly sophisticated and persistent threat campaigns against the federal government's IT architecture demonstrate that conventional perimeter-based defenses may not effectively protect critical systems and data. These threats have necessitated a government-wide shift from reliance on a 'moat protecting the castle' approach—a single-security perimeter—toward a 'zero trust' approach to cybersecurity based on continual verification of each user, device, application, and transaction.

As Forrester notes, "Zero Trust is not one product or platform; it's a security framework built around the concept of 'never trust, always verify' and 'assuming breach.' Attempting to buy Zero Trust as a product sets organizations up for failure."⁸ The framework includes people, processes, and technology. There is no silver bullet to achieve zero trust. Rather, it is an ongoing process that organizations must undertake to continuously improve access protections to their data, assets, applications, and services.

Similarly, as described by the National Institute of Standards and Technology (NIST):

Zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different—or no more trustworthy—than any non-enterprise-owned environment. In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications/services) . . . as well as continually authenticating and authorizing the identity and security posture of each access request.⁹

Simply put, ZTA moves defense of IT architectures from static, network-based perimeters to a dynamic approach focused on users, assets, and resources.

⁷ IT develops, maintains, and uses computer systems, software, and networks for the processing and distribution of data. It is centered on front-end informational activities such as email, finance, and human resources. OT is hardware and software that detects or causes a change through the direct monitoring and/or control of industrial equipment, assets, processes, and events. Many OT systems are part of critical assets the Agency uses to test rocket propulsion systems, control and communicate with spacecraft, and operate ground support facilities. Other OT systems are associated with infrastructure supporting these systems like electrical power, gas lines, and heating and cooling systems.

⁸ Steve Turner, "Zero Trust Is Not A Security Solution; It's A Strategy," *Forrester* (blog), February 18, 2021, <https://www.forrester.com/blogs/zero-trust-is-not-a-security-solution-it-is-a-strategy/>. Forrester is a global business and technology consulting firm that coined the concept of zero trust in 2009.

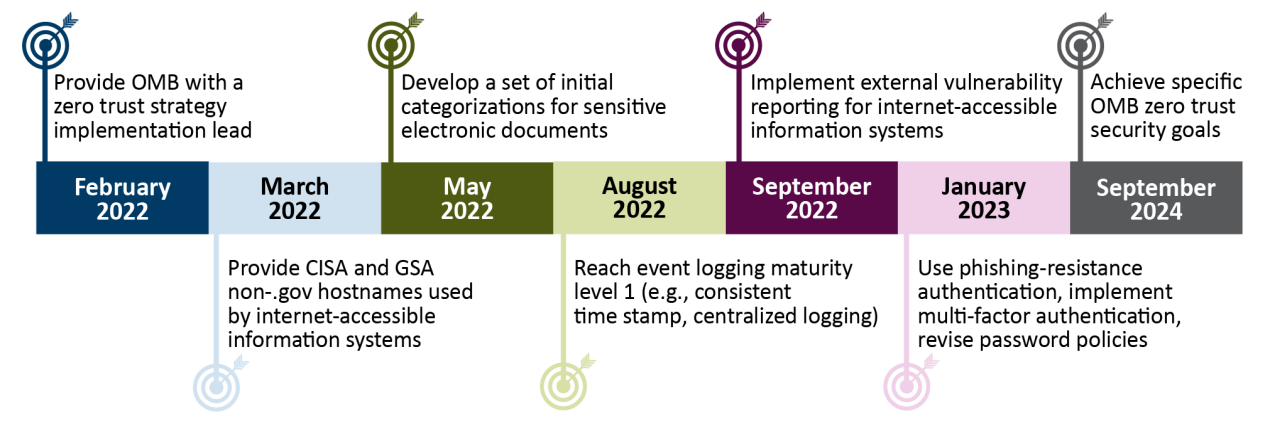
⁹ NIST Special Publication 800-207, *Zero Trust Architecture* (August 2020). Authentication verifies the identity of a user, process, or device as a prerequisite to allowing access to an information system.

Zero Trust Federal Mandates

Following several cyber incidents, the federal government established multiple zero trust requirements to modernize and implement stronger security standards government-wide. In August 2020, NIST issued a special publication on ZTA, providing a generalized roadmap for federal agencies to transition to a ZTA cybersecurity posture, from planning to deployment.¹⁰ In May 2021, the President issued Executive Order 14028, initiating a government-wide effort to ensure baseline security best practices are in place and federal agencies are migrating to ZTA.¹¹

In January 2022, OMB issued requirements for federal agencies to achieve specific zero trust security goals by the end of fiscal year 2024.¹² The memorandum provides a plan for moving the federal government to a ZTA cybersecurity model. This approach does not presume any person or device inside an organization’s perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data. The memorandum also requires agencies to appoint a zero trust strategy implementation lead and complete 19 tasks by September 30, 2024. Figure 1 shows the key ZTA milestones agencies were required to meet.

Figure 1: Key Zero Trust Architecture Milestones (as of January 2022)



Source: NASA Office of Inspector General (OIG) presentation of required milestones outlined in OMB M-22-09.

Note: Cybersecurity and Infrastructure Security Agency (CISA) and U.S. General Services Administration (GSA).

To begin the transition to ZTA and meet federal requirements, in February 2022 NASA appointed the Identity, Credential, and Access Management Architect within the Office of the Chief Information Officer (OCIO) as its zero trust strategy implementation lead (in December 2022, this role was reassigned to the Enterprise Cybersecurity Architect). Following this appointment, the Agency submitted in March 2022 the first version of its zero trust strategy implementation plan to OMB and the Cybersecurity and Infrastructure Security Agency (CISA). NASA provided OMB and CISA further ZTA updates in June 2022 and February 2023. For more information on OMB’s 19 agency ZTA tasks and NASA’s status on each of those requirements, see Appendix B.

¹⁰ NIST Special Publication 800-207.

¹¹ Executive Order 14028, *Improving the Nation’s Cybersecurity* (May 12, 2021).

¹² OMB M-22-09.

Subsequently, in July 2024, OMB issued additional guidance requiring federal agencies to submit an updated zero trust strategy implementation plan within 120 days of the date of the memorandum.¹³ The submission requires agencies to demonstrate how they are reducing risk by increasing the maturity level of information systems, which includes high value assets and high impact systems, in each of the five pillars—identity, devices, networks, applications and workloads, and data—outlined in CISA’s Zero Trust Maturity Model.¹⁴ Further, agencies must document current and target maturity levels to be achieved by the end of fiscal year 2026 for those information systems.

Zero Trust Principles, Pillars, and Stages of Maturity

In the realm of cybersecurity, the zero trust framework stands as a defense mechanism against evolving threats. Central to its efficacy are the principles of identity and access management, which redefine traditional security models that rely on perimeter-based security—allowing users or devices to move freely within the network once access is granted. Instead, the zero trust approach focuses on the perpetual verification of users, devices, and resources. Identity verification, facilitated by multi-factor authentication (MFA)—the process of verifying the identity of a user using two or more factors as prerequisites to access an IT system—and behavioral analytics, lies at the heart of this approach, ensuring that access requests are scrutinized for legitimacy.¹⁵

A zero trust solution requires operational capabilities that:

- **Never trust, always verify.** Treat every user, device, application, and data flow as untrusted. Using dynamic security policies, authenticate and explicitly authorize each to least privilege—granting a user only those permissions needed to perform their job.¹⁶
- **Assume breach.** Operate and defend resources with the assumption that an adversary already has a presence within the IT environment. Deny access by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all system configuration changes, resource accesses, and network traffic for suspicious activity.
- **Verify explicitly.** Access to all resources should be conducted in a consistent and secure manner to derive confidence levels—the degree of certainty that a digital identity corresponds to a real-world person—for access decisions to resources. Figure 2 highlights the differences between the traditional cybersecurity model and ZTA in four focus areas.



¹³ OMB Memorandum M-24-14, *Administration Cybersecurity Priorities for the FY 2026 Budget* (July 10, 2024).

¹⁴ CISA, *Zero Trust Maturity Model, Version 2.0* (April 2023). High value assets and high impact systems are IT systems in which at least one security objective (confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards Publication 199 potential impact value of “High.” NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), defines the potential impact as High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

¹⁵ Examples of MFA factors include asking for a PIN number or password, sending a confirmation text to a mobile phone, and using a fingerprint or face scan. Behavioral analytics is a method of analyzing user data to understand how people interact with digital products and services. It can be used to enhance IT security.

¹⁶ A dynamic security policy adapts and adjusts automatically to changing circumstances like evolving cyber threats.

Figure 2: Cybersecurity Approach—Traditional versus Zero Trust

FOCUS AREAS	TRADITIONAL 	ZERO TRUST 
Identity Management ^a	static, perimeter-based	dynamic, perimeter-less
Security Analytics ^b	once identified, implicit trust within perimeter	continuous confirmation of user identities within perimeter
Endpoint Protection ^c	authenticate to connect to network	authenticate to connect to network resources
Encryption ^d	unencrypted internal network traffic	all network sessions encrypted end-to-end

Source: NASA OIG presentation of information from Government Accountability Office, *Science & Tech Spotlight: Zero Trust Architecture* ([GAO-23-106065](https://www.gao.gov/products/GAO-23-106065), November 2022).

^a Identity management grants access to certain network resources at certain times based on user information. MFA is one method to determine that a specific user is entitled to access.

^b Security analytics uses threat intelligence, activity logs, traffic inspection, and other information about the network and its resources to detect unusual patterns that could warrant further investigation.

^c Endpoint protection ensures that devices (the endpoints) and their data are protected from threats and attacks. This may include monitoring for intrusion, known vulnerabilities, and malware.

^d Encryption prevents unauthorized data disclosure, modification, and access.

According to CISA’s Zero Trust Maturity Model, ZTA is composed of five key pillars:

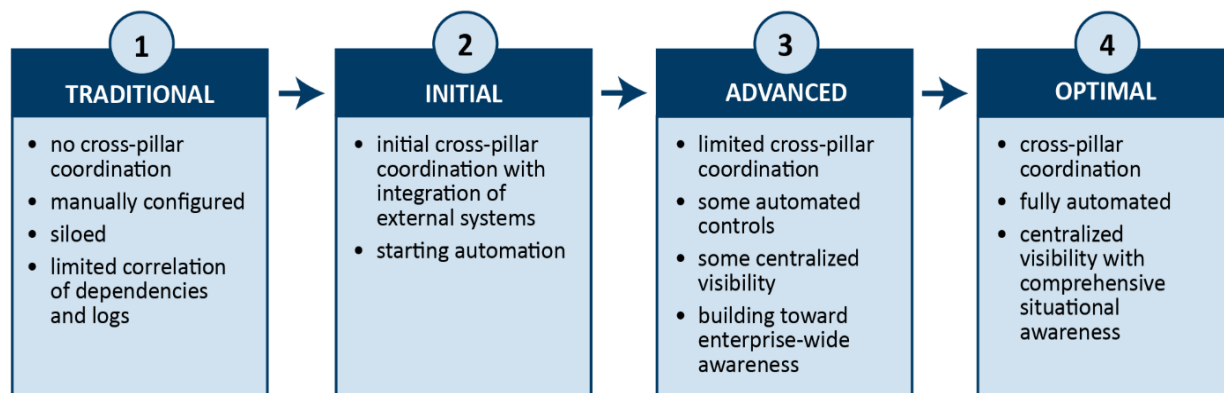
1. **Identity.** Refers to attributes that uniquely describe an agency user or entity, including non-person entities. Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose.
2. **Devices.** Includes assets that can connect to a network, such as servers, desktop computers, laptop computers, printers, and mobile phones. Agencies should have the ability to identify, authenticate, authorize, inventory, isolate, secure, remediate, and control all devices.
3. **Networks.** Segments, isolates, and controls networks—including agency internal networks, wireless networks, and the internet—both on and off premises with granular access (permitting or restricting access per-user, per-group, or per-resource) and policy restrictions.
4. **Applications and Workloads.** Manages and secures applications and workloads, which include agency systems, computer programs, and services performed on premises, on mobile devices, and in cloud environments.
5. **Data.** Protects critical data, assets, applications, and services. Agencies should inventory data, protect data at rest or in transit, and deploy mechanisms to detect and stop the theft of data.

Not all ZTA pillars can be achieved simultaneously. As a starting point, identity and devices are the two most critical pillars—the first line of defense in making sure no unauthorized user or device has access to IT systems. Identity verification ensures users have the right access needed to perform their job while limiting their access to functions not required. For devices, instead of verifying a user, the hardware of the device connected to a network is authenticated. Significantly, if unauthorized users or devices can access the network, the remaining pillars are compromised.

Implementing zero trust takes time and effort—it cannot be implemented overnight. For many systems, existing IT infrastructure can be leveraged and integrated to incorporate zero trust concepts, but the

transition to a mature ZTA often requires deploying additional capabilities like robust analytics to obtain the full benefits of a zero trust environment.¹⁷ As depicted in Figure 3, zero trust implementation matures over time, with enhanced visibility and automated responses allowing agencies to keep pace with threats.

Figure 3: CISA Zero Trust Stages of Maturity



Source: NASA OIG presentation of CISA's Zero Trust Maturity Model.

Challenges Implementing Zero Trust

As with any new strategy, implementing zero trust can present organizational challenges:

- Infrastructure compatibility.** It can be difficult for an organization with an outdated, or legacy, infrastructure to implement zero trust principles. Aligning existing systems with zero trust requirements can strain resources and increase complexities for IT teams. For example, ensuring intrusion prevention systems function with legacy systems could be challenging as newer technologies may not be designed to work with older systems, particularly in organizations with large investments in traditional technologies.
- Complexity of implementation.** Adopting a zero trust framework generally results in a significant overhaul of an organization's security policies and technologies. This, in turn, can challenge an organization when implementing zero trust principles and continuously managing security policies and technologies. For example, implementing new technologies like artificial intelligence and machine learning for automated threat detection impacts organization security policies.
- Balancing security needs with user convenience.** An organization must balance stringent security measures and user convenience. Without this balance, users will tire of repeatedly reauthenticating themselves. When security measures are too strict, frustrated users are more likely to seek out security workarounds that create new problems and introduce new risks. For example, while solutions like single sign-on attempts to balance user needs with more streamlined security control implementations, it is not feasible for every system.

¹⁷ Analytics provides insight into user and system behavior by observing real-time communications between all zero trust components.

- **Continuous monitoring and analytics.** Zero trust depends on the continuous monitoring of user and device behavior, which means it will generate lots of data. The organization must then analyze this data in a timely manner and respond to any security incidents it detects, which requires new threat intelligence capabilities. For example, new threat intelligence capabilities will need to flag suspicious events and remediate threats prior to causing damage to the organization.
- **Costs.** The adoption of zero trust often results in increased upfront costs. These costs can include investing in new technologies, hiring skilled personnel, and conducting trainings. For example, ZTA is an unfunded requirement where implementation costs are unknown. Therefore, collaboration on technical requirements and operational constraints is needed in organizations to ensure limited resources (money and personnel) are used efficiently.

Technical Debt and Legacy Systems

Further complicating zero trust is technical debt and how ZTA implementation will impact legacy systems. Technical debt—the cost of neglecting or delaying modernization of outdated (or legacy) systems—is an inevitable aspect of an organization’s operations.¹⁸ The aim is not to eliminate the technical debt of legacy systems entirely. That would require allocating significant resources toward remediation, hindering other facets of the organization. However, technical debt must be managed strategically to lessen the impact of future changes to systems and maintain long-term cybersecurity health. Examples of technical debt include the following:

- **Dated IT security systems.** Older security systems, including outdated firewalls, antivirus software, and intrusion detection systems, may not effectively protect against newer cyber threats.
- **Unsupported operating systems.** Running servers or desktop computers on unsupported operating systems that no longer receive security updates and patches expose security vulnerabilities and compatibility issues.
- **Obsolete hardware.** Using old hardware that cannot support newer software or operating systems can lead to performance bottlenecks, increased downtime, and higher maintenance costs.
- **Vulnerabilities from custom-built applications.** Custom applications built on older programming languages or platforms are difficult to maintain, update, and integrate with modern applications.
- **Outdated database systems.** Continued reliance on older database systems can limit performance, scalability, and integration with new applications.
- **Old financial systems.** Older financial software or enterprise resource planning systems that are not integrated with other business functions can lead to inefficiencies in data processing and financial reporting.¹⁹

¹⁸ Technical debt is accrued by neglecting or delaying modernization of technology devices, such as computer systems, servers, and applications.

¹⁹ Enterprise resource planning is a software system used to manage and streamline an organization’s functions, processes, and workflows in multiple areas, such as finance, human resources, supply chain management, and procurement, using automation and integration.

Use Case ZTA Best Practices

When it comes to cybersecurity, theoretical knowledge and practical application do not often go hand in hand. Therefore, to address some of the challenges of implementing ZTA, use cases should be created as pathfinders for specific systems or missions.²⁰ According to best practice, piloting use cases defines the context needed to understand ZTA integration throughout the IT ecosystem. Use cases validate IT resources ensuring critical mission and business processes are identified and tested and any issues are resolved prior to implementation.

NASA Organizational Boundaries and ZTA Approach

NASA is headquartered in Washington, DC, and supported by 10 centers and accompanying facilities across the United States. Various missions, programs, projects, and centers at NASA are treated as separate “organizations,” each operating within their own boundaries in areas such as IT responsibility, resources, and strategy. IT is managed as a joint responsibility between the OCIO and NASA mission directorates, centers, and headquarters offices. Specifically, the mission directorates, centers, and headquarters offices have responsibility for the software applications, while the OCIO has overarching responsibility for ensuring alignment of those applications with the NASA enterprise architecture and for all aspects of the IT infrastructure in which those applications reside.²¹

In 2024, NASA’s OCIO was responsible for approximately 51.3 percent of the Agency’s IT assets (desktop computers, laptop computers, and servers). The remaining 48.7 percent fell to the mission directorates and centers. While the Chief Information Officer has overarching responsibility for all aspects of the IT infrastructure, coordination with mission directorates and centers on IT matters ensures the Agency uses IT to improve government operations under federal Electronic Government initiatives, like ZTA.²² NASA’s five mission directorates—Aeronautics Research, Exploration Systems Development, Science, Space Operations, and Space Technology—are responsible for the Agency’s aeronautical efforts, human exploration systems development for lunar and Mars exploration, science missions, continuous presence of humans in space, and new technology developments. Notably, each of these organizations maintain their own independently managed IT, including, but not limited to, budget, staff, contracts, and IT hardware and software.

Additionally, NASA employs a board structure to integrate strategic, tactical, and operational decisions across the Agency. These boards, such as the Executive Council and Mission Support Council, provide strategic support and a framework for direction and decision-making.²³ The OCIO also has multiple governance and technical boards that make decisions on a variety of IT-related issues including data governance and IT strategy, policy, and management.

²⁰ Within IT, a use case is a set of possible sequences of interactions between users and a system to achieve a specific outcome; pathfinders represent a simplified task or workflow to demonstrate functionality and permit course-corrections as needed.

²¹ Enterprise architecture is a blueprint of IT assets, business processes, and governance principles used to create a unified and standardized hardware and software environment.

²² Electronic Government uses IT to improve and transform the effectiveness, efficiency, and service quality of government operations. Examples of Electronic Government initiatives include ZTA, online portals and websites, digital identity and authentication systems, and cybersecurity and data protection.

²³ The Executive Council serves as the Agency’s senior decision-making body. The Mission Support Council assesses and determines mission support requirements to enable the successful accomplishment of the Agency’s mission.

NASA's ZTA initiative is led by the Senior Agency Information Security Officer in their role as the Chief of the OCIO's Cybersecurity and Privacy Division, while the projects and initiatives that will deliver the Agency's ZTA technical capabilities are managed by the Cyber Improvement Portfolio (CIP) within the OCIO's Enterprise Project Management Office. CIP focuses exclusively on projects and initiatives that mitigate cybersecurity risks and achieve compliance with federal mandates—one of which is to deliver a ZTA. CIP identifies and tracks federal mandates according to technical and operational requirements and whether the task is funded or unfunded. The ZTA initiative is an unfunded federal mandate; NASA, like other federal agencies, did not receive funding to implement this complex architecture.

NASA's IT architecture is divided into three distinct environments: (1) corporate, (2) mission, and (3) Jet Propulsion Laboratory (JPL).²⁴ Corporate systems are managed by the OCIO, while mission and JPL systems are managed independently from the OCIO.²⁵ The Agency is addressing ZTA implementation in phases. Currently, NASA's ZTA efforts are focused solely on corporate systems. Implementation for non-corporate mission and JPL systems has not begun and is intended to follow in subsequent years.

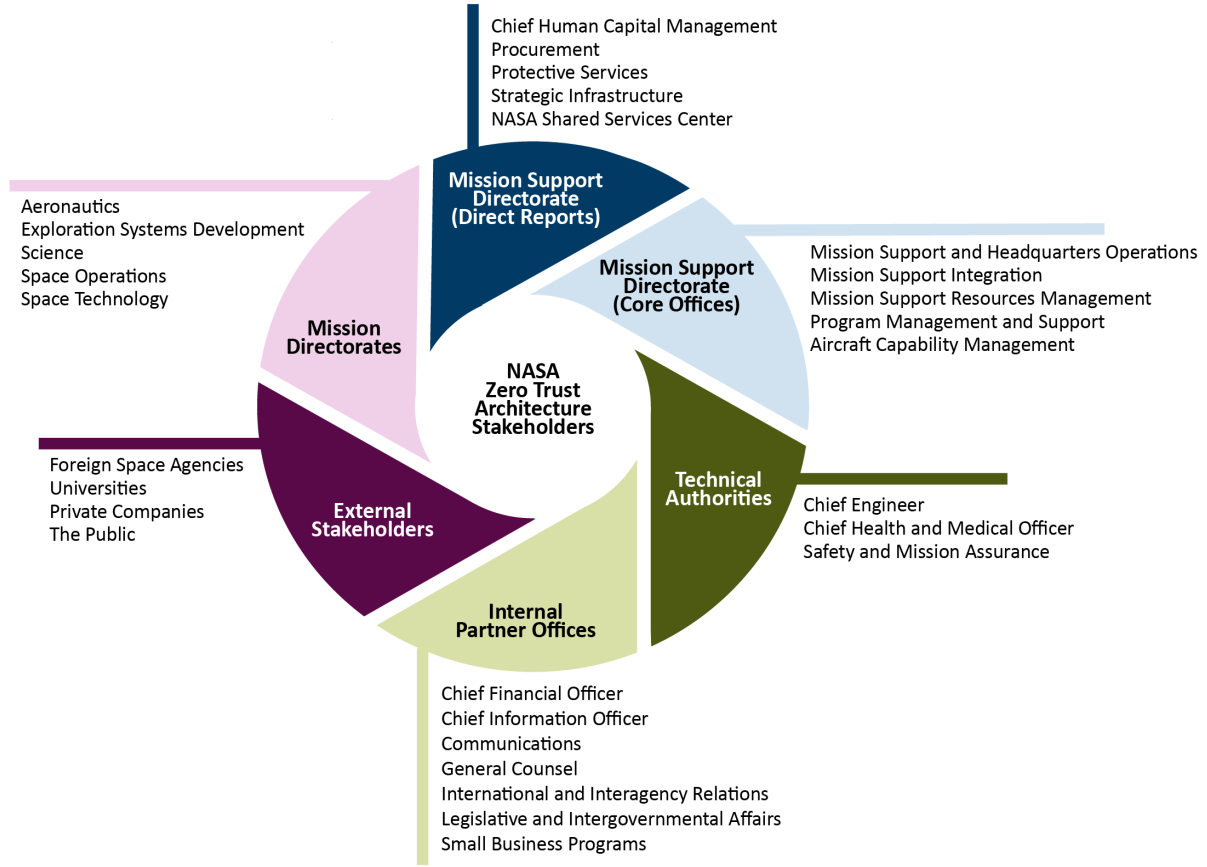
NASA has taken multiple actions for ZTA including appointing a zero trust strategy implementation lead, submitting its implementation plan to OMB, and establishing endpoint detection and external vulnerability reporting. For more details on the status of NASA's ZTA implementation tasks, see Appendix B. The OCIO is funding corporate ZTA initiatives, with an estimated budget of about \$211 million for fiscal years 2024 through 2029. Mission and JPL system owners are responsible for their individual funding, and monetary costs remain unknown for these systems.

There are also numerous stakeholders with vested interests in OCIO's ZTA initiative, each with different implementation expectations. As shown in Figure 4, key stakeholders include NASA organizations and employees, external partners, and the public.

²⁴ JPL is a research and development laboratory federally funded by NASA and managed by the California Institute of Technology.

²⁵ For purposes of this report, we included center systems under the mission environment, and the mission and JPL environments are collectively referred to as the non-corporate environment.

Figure 4: NASA Zero Trust Architecture Stakeholders (as of January 2025)



Source: NASA OIG presentation of Agency information.

NASA'S SHIFT TO ZTA IS PROGRESSING BUT LACKS AN AGENCY-WIDE FOCUS

NASA has made progress implementing a ZTA strategy within its corporate environment by appointing a zero trust strategy implementation lead, submitting its implementation plan to OMB, and completing ZTA security actions. However, ZTA implementation for mission and JPL systems has not yet started. By focusing on the corporate environment and delaying these systems to later phases, we found NASA's ZTA strategy lacks an Agency-wide focus. As a result, NASA is missing an opportunity to address enterprise-wide issues such as organizational boundaries, integration hurdles, and operational complexities that will impact ZTA adoption within the non-corporate environment. Utilizing this staged approach also means the total costs for this initiative remain unknown. What is more, NASA's decision to implement ZTA without intra-agency collaboration will likely mean its efforts will encounter a wide range of technical challenges due to the operational complexities of each mission directorates' unique environments.

Organizational Boundaries Limit Collaboration

Best practices dictate that governing boards and senior management exercise an active role in directing, evaluating, and monitoring IT operations, projects, and cybersecurity.²⁶ The effectiveness of IT management processes depends, in large measure, on the engagement and collaboration between senior management and other stakeholders. Collaboration is considered a crucial aspect of successful IT management because it allows teams to leverage diverse skill sets, share knowledge effectively, solve complex problems more efficiently, and ultimately achieve better outcomes by combining different perspectives and expertise, leading to increased innovation and productivity within IT projects.

We found a lack of effective engagement between the OCIO and mission directorates is hindering the implementation of ZTA Agency-wide. This is largely due to the OCIO and mission directorates operating within their organizational boundaries and not consistently collaborating or communicating. Additionally, limited IT-related representation from mission directorates and centers on OCIO decision-making boards and a lack of clear lines of authority on IT matters within each mission directorate further complicates the issue. Despite owning and being responsible for almost 50 percent of the Agency's IT assets, mission directorate and center officials told us that conversations with the OCIO's CIP ZTA team is limited because of "diffused responsibilities." Specifically, IT areas such as cybersecurity, cloud computing, and network services are managed jointly by the OCIO, mission directorates, and centers, with each focused on the systems that fall under their purview. This means that no single entity has insight or purview over individual IT areas. When needed communication between the OCIO, mission

²⁶ Best practices excerpted from NASA Office of Inspector General, *NASA'S Efforts to Improve the Agency's Information Technology Governance* (IG 18-002, October 19, 2017); NIST CSWP 29, *The NIST Cybersecurity Framework (CSF) 2.0* (February 26, 2024); and The Institute of Internal Auditors, *Global Technology Audit Guide: Auditing IT Governance* (July 2012).

directorates and centers is limited, this contributes to inefficient outcomes and delays in ZTA implementation.

Both OCIO and mission directorate officials described difficulty working across corporate and mission directorate boundaries generally due to organizational silos. Stakeholders explained that most coordination happens ad hoc in a bottom-up fashion, meaning coordination happens at the individual project level rather than with senior mission directorate management. We found no clear authority at the senior mission directorate level to coordinate ZTA initiatives with the OCIO. Consensus among stakeholders we interviewed was clear: IT deployments should be coordinated using a top-down approach to help decision-makers fully understand the opportunities and risks when transitioning to ZTA. Agreeing with stakeholder sentiment, OCIO officials acknowledged that an agency-centric approach is needed to influence the operational change required for ZTA. Modeled after a 'Technical Authority,' OCIO officials suggested that, perhaps, creating an 'IT Authority' would assist in getting the right engagement and expertise to drive change.²⁷

Recent outcomes of other IT enterprise-wide OCIO initiatives have provided mixed results, serving as lessons learned for implementing highly technical initiatives such as ZTA. For the OCIO, we found their communications with mission directorates was inconsistent—sometimes the OCIO engaged mission directorates early when implementing new initiatives, other times sporadically or not at all. For example, Executive Order 14028 required federal agencies to adopt multi-factor authentication (MFA) and encryption for data at rest and in transit. Mission directorate officials told us the OCIO clearly communicated and defined for them the MFA and encryption goals in the order, provided timelines for implementation, and followed up to ensure adherence to the order. Additionally, the OCIO communicated with mission directorates on the enterprise migration of mobile device management from IBM's *MaaS360* solution to the *Intune* software application.²⁸ The OCIO advised them about the switch to *Intune*, provided clear and concise directions on how the transition was going to happen, and followed up to ensure there were no issues. Early stakeholder engagement played a crucial role in MFA, data at rest and in transit encryption, and *Intune* implementation success. Stakeholders had the opportunity to supply context, identify kinks, and provide a voice to potential issues. Such stakeholder involvement mitigates risk, builds trust, and supports adjustments, which reduces cost and increases the chance of project success.

Conversely, there have been other Agency-wide initiatives where mission directorate officials expressed concern with the level of communication from the OCIO. For example, the OCIO implemented *Follow Me Print* to enable printing to any enterprise-managed multi-function device (i.e., printer) at any center. However, according to officials we interviewed, the OCIO's lack of outreach and collaboration with the mission directorates led to confusion about the transition and process. Unlike MFA and *Intune*, OCIO did not use any pathfinders (use cases or pilot programs) for *Follow Me Print*. In another example, mission directorate officials said they were not given notification prior to the OCIO disabling links embedded into

²⁷ The Technical Authority process is a part of NASA's system of checks and balances to provide independent oversight of programs and projects in support of safety and mission success through the selection of specific individuals with delegated levels of authority. Individuals with these formal delegations are Technical Authorities.

²⁸ *Intune* is used to protect NASA-related information and assets and reduce potential risks for mobile devices accessing NASA systems. Significantly, *Intune* uses Microsoft *Outlook* for NASA email, including encrypted email which meets the intent of Executive Order 14028.

drawings made with Adobe products to strengthen the application’s security, which impacted and slowed down Artemis II engineering activities.²⁹

Ultimately, organizational boundaries can further complicate ZTA implementation plans as well as cybersecurity strategies as a whole. Mission directorate officials cited a recent example of a cybersecurity vulnerability incident that was reported only across internal OCIO email distribution groups. Although the Science Mission Directorate’s Space Mission Operations project cybersecurity team (a group outside of the OCIO organizational boundary) identified and reported the incident, which affected the directorate’s NASA Communications Network (NASCOM), stakeholders were not informed of the problem.³⁰ Furthermore, remediation efforts and reporting comprised solely of OCIO-led cybersecurity groups, excluding the Space Operations Mission Directorate, who are the primary users of NASCOM.

Organizational boundaries and silos can hinder collaboration and the sharing of best practices needed for ZTA adoption. The transition to ZTA must be carefully orchestrated, requiring a concerted, deliberate, and holistic “all-of-agency” approach. Until long-standing challenges of coordinating IT and cybersecurity requirements across corporate and non-corporate boundaries are addressed, enterprise-wide implementation of ZTA will be delayed.

Integration Hurdles Hinder ZTA Initiatives

While the foundation of a zero trust strategy is the existing IT infrastructure, integrating NASA’s various IT ecosystems to establish a cohesive zero trust framework is challenging. A diverse federated IT environment, disparate stakeholders, and legacy systems add layers of complexity to the integration process. By delaying the transition of mission and JPL systems to later phases in the ZTA implementation process, the Agency missed an opportunity for knowledge sharing and the understanding needed for ZTA integration within its complex, non-corporate environment.

Diverse Federated IT Environment

NASA operates under a federated model with subordinate organizations across the Agency, such as mission directorates and centers, that retain decision authority and budgets for their respective efforts. Headquarters—in this case the OCIO—provides Agency-wide coordination of IT efforts, like ZTA. To advance science, space exploration, technology, and aeronautics missions, NASA’s federated environment is diverse and complex. As a result, many of the challenges and constraints mission system owners face to secure IT assets are often not apparent or visible to the OCIO.

For example, implementing ZTA’s identity pillar—such as using MFA for identity management—for mission systems can be technically difficult for projects and facilities like the International Space Station

²⁹ Artemis II will be the first crewed flight test of the Space Launch System heavy-lift rocket and Orion Multi-Purpose Crew Vehicle around the Moon.

³⁰ Managed out of Goddard Space Flight Center, NASCOM provides terrestrial communications between ground stations, mission control centers, and other elements of spacecraft ground segments, providing worldwide, near real-time transmission of commands, telemetry, voice, and television signals.

and Huntsville Operations Support Center that involve international and other external partners.³¹ MFA can be challenging between NASA and external partners due to data ownership, classification, and privacy issues. Highly sensitive data might require stricter access controls and additional encryption compared to less critical data necessitating customized zero trust policies. Additionally, contractors may use IT systems not under the purview of NASA making system and user verification impractical.

During our review, a prevalent concern expressed by mission directorate officials was that they were not consulted about ZTA during early planning and were unsure if the OCIO was aware of interoperability issues unique to mission and center environments. A “push-pull” relationship exists between the OCIO and mission directorates and centers mainly due to the OCIO’s unfamiliarity with mission directorate and center operational processes, making ZTA integration difficult. By and large, officials from each mission directorate told us they want to be included in the early stages of ZTA implementation to identify and collaboratively work through potential problems. For example, Science Mission Directorate officials said they could have easily provided a wide variety of projects, such as the Hubble Space Telescope, James Webb Space Telescope, and high-end computing activities, to use as pathfinders to demonstrate ZTA and resolve issues early.³² These pathfinders could have offered valuable insights for identifying and resolving integration conflicts within unique mission-specific environments. However, the mission directorates were not asked.

OCIO officials explained they are spearheading ZTA within the corporate environment first to positively influence mission directorate adoption through their own successes. While we understand this gradual implementation approach, in our view, by relegating mission and JPL environments to later ZTA phases, an opportunity was missed to identify and evaluate use cases—descriptions of how a user interacts with a system—prior to broader ZTA implementation.

Disparate Stakeholders

In addition to the diverse federated IT environment, NASA works with a variety of stakeholders, including contractors and international partners, which further complicates ZTA implementation. This is particularly the case with implementing MFA. In fiscal year 2023, the White House called upon agencies to accelerate their zero trust implementation by replacing password authentication with MFA. As one of the central tenets of ZTA, identity and device authentication introduces strict enterprise-wide security policies that impact stakeholders’ access to Agency resources. While NASA has begun to implement ZTA in the corporate environment, the Agency faces challenges within the non-corporate environment, especially with identity management given the need to share scientific data with its stakeholders. In discussions with mission directorate officials, the requirement for stakeholders to use a smartcard—the federal government and NASA’s preferred method to implement MFA—was cited as a top identity management concern as shown in the following examples:

³¹ The Huntsville Operations Support Center at NASA’s Marshall Space Flight Center is a multi-program mission operations facility supporting the International Space Station, which includes working with international partners and researchers on science payloads; the Space Launch System, which includes external contractor laboratories from The Boeing Company; and small satellite missions and other small projects.

³² The Hubble Space Telescope, launched in 1990, is a space-based observatory providing important discoveries and science to advance understanding of the cosmos. The James Webb Space Telescope, launched in 2021, is a large orbiting infrared observatory operating a million miles from Earth that is studying the origins of the universe. High-end computing, or supercomputing, provides the critical processing power and time-saving capabilities that allow NASA to gain insight from large amounts of data that would take traditional computers much longer to assess.

- **External partners.** In lieu of providing partners a smartcard—a personal identity verification card used to access facilities and systems—NASA provides an RSA token for authentication.³³
- **External laboratories.** Many unresolved questions remain regarding how to handle authentication for NASA’s external partners, such as The Boeing Company’s Space Launch System laboratory located at NASA’s Huntsville Operations Support Center. Currently, a mix of different authentication mechanisms are used at the facility. For example, some Boeing employees use NASA smartcards and computers while others use Boeing devices.
- **Contracts.** MFA was not a consideration when contracts such as the Space Launch System contract with The Boeing Company was written and awarded 10 years ago. This requires mission directorates to consider how they will handle non-contractual IT initiatives, like ZTA, that require additional costs and resources. For example, discussions are currently underway with the mobile launcher 2 contractor to determine how to implement MFA on the contractor’s network.³⁴

Mission directorate officials described independent processes used for access and identity management across their systems. While some mission systems use OCIO tools, such as Microsoft 365 and Active Directory, most systems have their own tools and computer security processes for identity and access management, authentication, and credentialing.³⁵ For instance, the OCIO manages network security of the NASA ground communications system—NASCOM—but leaves the computer security processes to the stakeholders who own the assets using NASCOM. Additionally, some customers are provided exemptions to run their own network segments—an architectural approach that divides a network into multiple subnets—creating confusion of where network boundaries are drawn and who is responsible for authenticating access to those resources. OCIO officials stressed the need for centralized identity management and credentialing to provide a solid foundation for ZTA across the Agency.

Despite the need to integrate access and identity management across the Agency, we found the OCIO struggled to assuage mission directorate officials’ concerns about authentication. Integrating stakeholder authentication into ZTA requires a nuanced approach. Collaborating early with stakeholders about MFA and other IT initiatives will help minimize mission disruptions and ensure interoperability as NASA moves toward an Agency-wide ZTA.

Legacy Systems

The technical debt of maintaining legacy systems can pose significant challenges. NASA uses legacy information technology (IT) systems—computer systems, software, and networks for activities like email, finance, and human resources to conduct Agency business. It also uses legacy operational technology (OT) systems—hardware and software that directly monitors and controls industrial equipment, assets, processes, and events to support operations. A legacy system, in the context of

³³ A personal identity verification card, also known as a smartcard or badge, includes an agency’s seal and return address; the full name, agency, photo, and physical characteristics of personnel; the card’s expiration date; and a serial number. RSA is an MFA technology used to protect network services. The RSA authentication mechanism consists of an assigned hardware or software token that generates a dynamic authentication number code at fixed intervals.

³⁴ The mobile launcher is the ground structure NASA uses to assemble, process, transport, and launch the integrated Space Launch System rocket and Orion Multi-Purpose Crew Vehicle system.

³⁵ *Microsoft 365* is a software, collaboration, and cloud-based service that provides productivity tools (e.g., *Word*, *Excel*), device management, and security. *Active Directory* is a Microsoft service that enables administrators to manage permissions and access to network resources by organizing users into logical groups and subgroups. Credentialing is the process of using login data, such as username and password, to verify a user’s identity and grant them access to a system.

computing, refers to the use of outdated computer systems, programming languages, and application software instead of more modern alternatives. While problematic due to compatibility issues with newer technology, obsolescence, or lack of vendor support, legacy systems continue to be used because they provide critical functions tied to mission objectives.

OCIO officials explained they must consider legacy or potentially outdated IT systems in the context of criticality to NASA's mission, technological obsolescence, ongoing operations, and maintenance costs, as well as the extent to which the system can meet IT security standards. For instance, SAP—NASA's financial management software—is a legacy corporate IT system in need of modernization as it is critical to the entire Agency. OCIO officials acknowledged the system will reach its end-of-life in the next few years and needs to be modernized. The goal of modernizing legacy systems is to ensure that IT infrastructure, including the new ZTA, supports current business needs and technological standards effectively.

Similarly, mission directorate officials told us legacy systems and end-of-life IT hardware and software “remain a sticky issue” as a legacy system does not, by default, equate to obsolete in the context of NASA missions. Generally, decisions on whether to remain status quo or upgrade an IT system depends on operational, technical, and financial constraints. For example, the Aqua spacecraft, part of NASA's Earth-observing satellite fleet that collects large amounts of information on water, completed its operational mission in December 2021, but continues to gather useful data while in free-drift mode outside of its historically maintained orbit. Likewise, the scientific community was utilizing legacy operating systems that are no longer supported by vendors. NASA must consider whether it is prudent to make technical upgrades and spend limited resources and money to update the systems. Currently, decision-makers in the OCIO and mission directorates lack the information needed to determine the fate of legacy systems within the context of ZTA.

Given the continued use of legacy systems, their criticality to ongoing and future missions, and the potential risk to ZTA implementation, an Agency-wide understanding of how legacy systems fit into the ZTA framework and ensuring their compatibility is essential. However, during our review, we found NASA does not have a centralized process to identify legacy IT and OT systems, nor does it maintain an authoritative source inventory of legacy IT and OT systems. Rather, legacy systems are left to the system owners to identify and manage risk through cybersecurity assessment and authorization, risk management, and budget processes. Without an Agency-wide program to identify, prioritize, and execute the updating, replacing, or retiring of legacy systems, migrating to ZTA will be delayed.

Delaying Mission Directorate and JPL ZTA Implementation Obscures Operational Complexities and Erodes Progress

The OCIO's current ZTA implementation plan for the corporate environment is robust. However, in its decision to implement ZTA using a staged approach without intra-agency collaboration, the OCIO missed an opportunity to fully address the Agency as a whole. Without a joint approach, the unique IT and OT operational complexities specific to the mission directorates and JPL will hinder OCIO's ZTA overall implementation progress. The absence of an Agency-wide ZTA approach makes overcoming operational and technical challenges more difficult due to the unique environments of mission directorates and JPL.

While IT is similar across multiple disciplines, there are facets of IT that differ completely. For example, the differences between supercomputers—used more prolifically by the mission directorates and JPL—and desktop computers are significant, driven by their intended use cases, architectural designs, and performance capabilities. Supercomputers are designed to perform complex calculations at incredibly high speeds, often measured in petaflops (quadrillions of calculations per second). In contrast, desktop computers are optimized for general tasks like web browsing and document editing. The technical expertise needed to operate the two systems is different—requiring specific training and understanding to properly manage each system to perform the functions they were designed for.

Additionally, the convergence of IT and OT presents several unique security challenges. Security solutions designed for IT systems may not be immediately transferable to the OT environment. Many legacy OT system components use small processors with limited computing capabilities, making it difficult to run even basic malware protection software or other security applications. OT components also tend to have long life cycles, which means embedded software may continue to operate long after the manufacturer has stopped providing support.

While the CIP ZTA team is providing encouraging results for corporate systems, non-corporate mission and JPL systems have not been adequately evaluated for ZTA technical, financial, and operational risks. The technology needed for ZTA adoption within the non-corporate environment—such as Software-Defined-Access, trusted connection protocols, and network monitoring on Linux- or Windows-based systems managed outside of the OCIO—have not been assessed by NASA subject matter experts.³⁶ Additionally, while the CIP ZTA team has forecasted an estimated budget in excess of \$211 million for fiscal years 2024 through 2029 to implement ZTA solutions within the OCIO, monetary costs were not evaluated and remain unknown for ZTA implementation on mission and JPL systems.

Most mission directorate officials we spoke with stated they were not asked to be a part of planning processes, nor were they consulted, for NASA's ZTA solution. Similarly, many of the mission directorate officials suggested if they had been involved, they would have been able to offer internal projects or mission-specific system environments to study and use as a pathfinding opportunity to test a planned ZTA method. For example, NASA's Space Communications and Navigation (ScAN) program benefited from past IT collaboration with the OCIO, yielding positive cybersecurity results.³⁷ Specifically, the OCIO actively engaged the ScAN program to ensure its systems were secure and adhered to best practices, providing a more secure cybersecurity environment after a concerted effort was made to work together. Despite this relationship, ScAN was not included as a potential pathfinder for ZTA implementation in the planning phase.

Mission directorate officials cited concerns about the potential operational impact of being left outside of the ZTA decision-making process. They noted the OCIO has limited knowledge of the technical complexities of implementing ZTA within the mission directorates' operational environment. For example, the OCIO is adopting metrics to measure the overall effectiveness of ZTA implementation without communicating to mission directorate officials the expectations or how the results will be derived. Mission directorate officials are concerned the metrics will be indiscriminately applied, both to

³⁶ Software-Defined-Access helps organizations enable policy-based automation from the network edge to the cloud. Trusted connection protocols provide guidance and an execution framework used to implement baseline boundary security standards. Network monitoring is the process of discovering, mapping, and tracking the health of a network across the hardware and software ecosystem.

³⁷ The ScAN program is responsible for the Agency's space communications operations. NASA and non-NASA missions rely on its two networks, the Near Space Network and Deep Space Network, to monitor Earth's weather and the effects of climate change, support lunar exploration, and explore the solar system and beyond.

legacy systems that are so old they will be physically unable to make the recommended upgrades, or to temporary systems, typical of scientific laboratory environments, which will lead to skewed monitoring results. Such operational complexities are not easily understood within the OCIO because they may not be familiar with the unique systems and subsets of systems that currently make up NASA's mission environment.

NASA's engineering and scientific research communities have long employed a "test like you fly" approach—a comprehensive assessment and testing process pre-launch that accurately reflects the planned mission profile—which impacts acquisition strategy, interactive product development, requirements definitions, systems engineering, fault analysis, and risk management. The idea of adopting such an approach is to ensure mission success and deliver a solution that is technically safe, sound, and meets the objective prior to launching a mission.

In our view, the same principle applies when it comes to the acquisition and implementation of new or upgraded IT and OT systems, as well as any changes that can impact either or both technology systems. The exclusion of mission directorate input and assessments during the planning and initial implementation of ZTA will likely create barriers to success and ultimately increase associated costs once the OCIO implements ZTA with mission and JPL systems.

CONCLUSION

Given the increasingly sophisticated and persistent threat campaigns against the federal government's IT architecture, OMB has directed a government-wide shift from reliance on a 'moat protecting the castle' approach—a single-security perimeter—toward a 'zero trust' approach to cybersecurity based on continual verification of each user, device, application, and transaction. With its unique mission and numerous public facing websites, NASA is a particularly attractive target to cyber criminals. Despite the potential benefits, NASA faces challenges migrating to an Agency-wide ZTA. Organizational boundaries and integration hurdles pose operational, technical, and financial complexities due to the non-homogeneous nature of the Agency's missions.

Although the OCIO has made progress implementing ZTA in the corporate environment, it is unlikely that a shift to an Agency-wide ZTA that includes mission and JPL systems can be realized in the near term. As a result, there may be an indefinite period when ZTA is implemented on portions of NASA's IT infrastructure that coexists with systems that have not implemented ZTA. While we appreciate that NASA must balance the nimbleness and creativity provided by local control of systems (mission directorates and JPL) with the efficiency and interoperability of systems provided by centralization (enterprise-wide management by the OCIO), delaying implementation of the non-corporate environment impacts Agency-wide cybersecurity and obfuscates the overall costs for the effort. Ultimately, the robustness of zero trust hinges on the ability to maintain a strong focus and collaborate on the implementation of ZTA across both corporate and non-corporate IT and OT systems.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To expand NASA's ZTA adoption and address organizational boundaries, integration hurdles, and operational complexities, we recommended the Associate Administrator and Chief Information Officer:

1. Collaborate with mission directorate officials to update NASA's ZTA implementation plan to include all efforts associated with the transition to ZTA within the non-corporate environment.
2. Develop a centralized process to track legacy systems that details deficiencies along with operational, technical, and financial constraints to determine a best course of action for remediation.
3. Embed OCIO subject matter experts within the mission directorates to provide Agency-focused advocacy and expertise to analyze mission system cybersecurity compatibility and operational complexities.
4. Engage mission directorates as ZTA pathfinders to identify and evaluate early adoption use-case candidates, employ a "test like you fly" approach, and provide insight to potential issues.

We provided a draft of this report to NASA management who concurred or partially concurred with our recommendations and described planned actions to address them. We consider management's comments responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

Management's comments are reproduced in Appendix C. Technical comments provided by management and revisions to address them have been incorporated as appropriate.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Robert H. Steinau
NASA OIG Senior Official

APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from April 2024 through January 2025 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.

We assessed NASA's ZTA efforts, with a focus on three subject areas: (1) policy, (2) legacy systems, and (3) cybersecurity. To gain a holistic view of NASA's progress toward implementing the federal ZTA strategy and specific cybersecurity standards and objectives required by OMB M-22-09, we reviewed numerous federal and NASA policies, regulations, guidance, frameworks, and industry best practices. We met with the Chief Information Officer to understand how NASA prepared and revised its zero trust strategy implementation plan. We interviewed personnel from the OCIO, its Cybersecurity and Privacy Division, and others responsible for overseeing ZTA activities. We also met with multiple officials from the Mission Support Directorate, Aeronautics and Research Mission Directorate, Exploration Systems Development Mission Directorate, Science Mission Directorate, Space Operations Mission Directorate, and Space Technology Mission Directorate regarding the ZTA framework and potential pathfinder use cases.

Additionally, we determined whether legacy IT and OT systems have been identified and prioritized, as well as assessed the systems' operational complexities and cybersecurity challenges. Finally, we evaluated the OCIO's engagement across organizational boundaries and their collaboration with stakeholders to identify shortcomings that could affect Agency-wide ZTA implementation. Collectively, this informed our understanding and helped us assess the overall management of NASA's ZTA initiative.

Assessment of Data Reliability

We did not use data to materially support findings, conclusions, or recommendations to address the audit objectives.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations to determine ZTA and cybersecurity preparedness. Internal controls are dynamic processes designed to provide reasonable assurance that information is reliable, accurate, and timely. We considered the reviewed internal controls adequate and not significant to the ZTA audit objectives. Our recommendations, if implemented, will improve NASA's ZTA identified weaknesses.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General has not issued any reports of relevance to the subject of this audit. However, we noted ZTA in our November 2023 and 2024 Top Management and Performance Challenges reports. Additionally, the Government Accountability Office has issued an

ancillary report of interest to this topic. Unrestricted reports can be accessed at <https://oig.nasa.gov/> and <https://www.gao.gov/>, respectively.

NASA Office of Inspector General

2024 Report on NASA’s Top Management and Performance Challenges ([MC-2024](#), November 2024)

2023 Report on NASA’s Top Management and Performance Challenges ([MC-2023](#), November 2023)







Government Accountability Office









Science & Tech Spotlight: Zero Trust Architecture ([GAO 23-106065](#), November 2022)






APPENDIX B: NASA'S ZERO TRUST IMPLEMENTATION STATUS

On January 26, 2022, OMB issued memorandum M-22-09 establishing the government's ZTA strategy and requiring all federal agencies to implement 19 tasks by September 30, 2024. Table 1 provides the required tasks, including its related CISA Zero Trust Maturity Model pillar and a description of the task, as well as the agency action and due date for the task, the task's status (green is complete, yellow is in progress, and red is not yet addressed), and any other relevant information.

Table 1: NASA's Zero Trust Implementation Status (as of August 2024)

Task and Related Pillar	Task Description	Agency Action (Timeline and Due Date)	Task Status	Comment
1. General Direction	Agencies must submit to OMB and CISA an implementation plan for fiscal years 2022 to 2024 and a budget estimate for fiscal years 2023 and 2024.	Within 60 days. Due: March 2022		Implementation plan and budget estimate delivered on time. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a
2. Identity	Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.	Include in agency zero trust strategy implementation plan. Due: March 2022		Complete. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a
3. Identity	Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the second quarter of fiscal year 2029. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a
4. Identity	Public-facing agency systems that support multi-factor authentication must give users the option of using phishing-resistant authentication.	Within 1 year. Due: January 2023		Estimated completion in the fourth quarter of fiscal year 2026.
5. Identity	Agencies must remove password policies that require special characters and regular password rotation from all systems.	Within 1 year. Due: January 2023		Estimated completion in the fourth quarter of fiscal year 2028.
6. Identity	Agency authorization systems should work to incorporate at least one device-level signal alongside identity information about the authenticated user.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the fourth quarter of fiscal year 2027. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a

Task and Related Pillar	Task Description	Agency Action (Timeline and Due Date)	Task Status	Comment
7. Devices	Agencies must create ongoing, reliable, and complete asset inventories, including by leveraging the continuous diagnostics and mitigation program.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the first quarter of fiscal year 2025. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a
8. Devices	Agencies must ensure their endpoint detection and response tools meet CISA's technical requirements and are deployed and operated across their agency.	Agency implementation within 120 days as consistent with OMB M-22-01. ^b Due: May 2022		Complete.
9. Devices	Agencies must work with CISA to identify gaps, coordinate on deployment, and establish information sharing capabilities with CISA.	Agency implementation within 120 days as consistent with OMB M-22-01. ^b Due: May 2022		Estimated completion TBD.
10. Networks	Agencies must resolve Domain Name System queries using encrypted Domain Name System wherever it is technically supported.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion TBD.
11. Networks	Agencies must enforce authenticated HTTPS for all production HTTP traffic, including traffic that does not cross the public internet.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the first quarter of fiscal year 2025.
12. Networks	Agencies must work with the DotGov program at CISA to "preload" agency-owned .gov domains as HTTPS-only in web browsers.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the first quarter of fiscal year 2025.
13. Networks	Agencies must develop a zero trust architecture plan that describes how the agency plans to isolate its applications and environments, in consultation with CISA, and include it in the full implementation and investment plan required by OMB M-22-09.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the fourth quarter of fiscal year 2029. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a
14. Applications and Workloads	Agency system authorization processes must employ both automated analysis tools and manual expert analysis.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion TBD. Listed on Agency ZTA Roadmap, but has not yet been funded. ^a

Task and Related Pillar	Task Description	Agency Action (Timeline and Due Date)	Task Status	Comment
15. Applications and Workloads	Agencies must welcome external vulnerability reports for their internet-accessible systems.	Due: September 2022		Complete.
16. Applications and Workloads	Agencies must select at least one FISMA moderate system that requires authentication and is not currently internet accessible, and securely allow full-featured operation over the internet.	Within 1 year. Due: January 2023		Estimated completion TBD.
17. Applications and Workloads	Agencies must begin providing CISA and the U.S. General Services Administration any non-.gov hostnames used by their internet-accessible information systems.	Within 60 days. Due: March 2022		Estimated completion in the first quarter of fiscal year 2025.
18. Applications and Workloads	Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.	Include in agency zero trust strategy implementation plan. Due: March 2022		Requirement documented in implementation plan. Estimated completion in the first quarter of fiscal year 2025.
19. Data	Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise, with the goal of automatically monitoring and potentially restricting how these documents are shared.	Within 120 days. Due: May 2022		Estimated completion in the fourth quarter of fiscal year 2029.

Source: NASA OIG presentation of Agency and OMB M-22-09 information.

^a The Agency ZTA Roadmap provides the blueprint that outlines how NASA will implement ZTA.

^b OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 8, 2021).

APPENDIX C: MANAGEMENT'S COMMENTS

National Aeronautics and Space Administration

Office of the Administrator
Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001



March 14, 2025

TO: Assistant Inspector General for Audits

FROM: Associate Administrator

SUBJECT: Agency Response to OIG Draft Report, "Audit of NASA's Zero Trust Architecture" (A-24-08-00-MSD)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Audit of NASA's Zero Trust Architecture" (A-24-08-00-MSD), dated February 18, 2025.

On February 18, 2025, OIG issued the attached draft report titled, "Audit of NASA's Zero Trust Architecture" (A-24-08-00-MSD). In this report, the OIG found that Zero Trust Architecture (ZTA) is progressing but lacks an Agency-wide focus. NASA is missing an opportunity to address enterprise-wide issues such as organizational boundaries that limit collaboration, integration hurdles that hinder ZTA initiatives, and operational complexities that delayed Mission Directorate and NASA Jet Propulsion Lab (JPL) implementation.

The OIG makes four recommendations addressed to the Associate Administrator and Chief Information Officer (CIO) to expand ZTA's adoption and address organizational boundaries, integration hurdles, and operational complexities.

Specifically, the OIG recommends the Associate Administrator and CIO:

Recommendation 1: Collaborate with mission directorate officials to update NASA's ZTA implementation plan to include all efforts associated with the transition to ZTA within the non-corporate environment.

Management's Response: NASA concurs with this recommendation. The NASA Office of the Chief Information Officer (OCIO) will conduct a series of focus sessions with representatives from the Mission Directorates and JPL to capture and modify the current ZTA implementation plan to broaden its scope to include the full NASA Enterprise Information Environment, inclusive of Information Technology, Operational Technology, and Internet of Things.

Estimated Completion Date: June 26, 2026.

Recommendation 2: Develop a centralized process to track legacy systems that details deficiencies along with operational, technical, and financial constraints to determine a best course of action for remediation.

Management's Response: NASA concurs with this recommendation. NASA will develop a centralized process to capture the required data via periodic data calls until such time as the material can be moved to the Agency's Configuration Management Database (still under development). This effort will leverage low-code/no-code capabilities (i.e., Microsoft Power BI suite) to establish the central repository.

Estimated Completion Date: September 25, 2026.

Recommendation 3: Embed OCIO subject matter experts within the mission directorates to provide Agency-focused advocacy and expertise to analyze mission system cybersecurity compatibility and operational complexities.

Management's Response: NASA partially concurs with this recommendation. Having OCIO subject matter experts embedded with the missions would be ideal; however, current OCIO staffing constraints make this approach impractical. The OCIO has a Customer Engagement Office to engage with missions to help determine requirements and a Cybersecurity Mission Integration office to advise and provide targeted expertise for mission programs and projects. Missions are encouraged to bring on staff cybersecurity experts dedicated to fully explore operational complexities and ensure cybersecurity compatibility. To cover Information Technology, Operational Technology/Internet of Things, and Cybersecurity interoperability and operational complexities across each of the Mission Directorates and JPL, there may need to be workforce plus-ups and subject matter training/education to ensure optimal support from within these organizational units.

Estimated Completion Date: December 26, 2025.

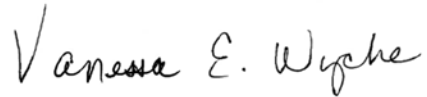
Recommendation 4: Engage mission directorates as ZTA pathfinders to identify and evaluate early adoption use-case candidates, employ a "test like you fly" approach, and provide insight to potential issues.

Management's Response: NASA concurs with this recommendation. As part of a previously planned series of facilitated workshops under the Digital Transformation initiative with the Mission Directorates and JPL to educate them on Zero Trust and to determine their Zero Trust implementation gaps (barriers, challenges), we would leverage these opportunities to address this recommendation.

Estimated Completion Date: September 26, 2025.

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

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

A handwritten signature in black ink that reads "Vanessa E. Wyche". The signature is written in a cursive style with a large initial 'V'.

Vanessa Wyche
Associate Administrator (Acting)

cc:
Chief Information Officer/Mr. Seaton

APPENDIX D: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Acting Administrator
 Acting Associate Administrator
 Acting Chief of Staff
 Chief Information Officer
 Associate Administrator for Mission Support Directorate
 Associate Administrator for Aeronautics and Research Mission Directorate
 Acting Associate Administrator for Exploration Systems Development Mission Directorate
 Associate Administrator for Science Mission Directorate
 Associate Administrator for Space Operations Mission Directorate
 Associate Administrator for Space Technology Mission Directorate

Non-NASA Organizations and Individuals

Office of Management and Budget
 Deputy Associate Director, Climate, Energy, Environment and Science Division

Government Accountability Office
 Director, Information Technology and Cybersecurity
 Director, Contracting and National Security Acquisitions

Office of Science and Technology Policy
 Deputy Director, Science and Society

Congressional Committees and Subcommittees, Chair and Ranking Member

Senate Committee on Appropriations
 Subcommittee on Commerce, Justice, Science, and Related Agencies

Senate Committee on Commerce, Science, and Transportation
 Subcommittee on Space and Science

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
 Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Government Reform
 Subcommittee on Government Operations

House Committee on Science, Space, and Technology
 Subcommittee on Investigations and Oversight
 Subcommittee on Space and Aeronautics

(Assignment No. A-24-08-00-MSD)