NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

# AUDIT OF NASA'S POLICY AND PRACTICES REGARDING THE USE OF NON-AGENCY INFORMATION TECHNOLOGY DEVICES

**August 27, 2020**

**Report No. IG-20-021**

# 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, D.C. 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/aboutAll.html.

NASA Office of Inspector General
Office of Audits

# RESULTS IN BRIEF

## Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices

August 27, 2020 IG-20-021 (A-19-010-00)

## WHY WE PERFORMED THIS AUDIT

Smartphones, tablets, and laptops are integral to the work of NASA employees and their contractor, academic, federal, and international partners. However, use of this equipment to connect to NASA non-public networks and systems increases opportunities for individuals and organizations to improperly access Agency data. Although NASA does not generally permit personally-owned mobile devices and laptops to access Agency networks and systems, certain authorized mobile devices and users are allowed to access NASA's enterprise email system if they adhere to specified business rules. Additionally, based on the terms of their respective agreements with NASA, partners may be allowed to use their own computers to access the Agency's enterprise and mission networks and systems with proper authorization.

For years, NASA permitted personally-owned and partner-owned information technology (IT) devices to access non-public data through its networks and systems, even if those devices did not have a valid authorization. In April 2018, the Chief Information Officer (CIO) clarified existing NASA requirements to disallow connection of personally-owned and partner-owned IT devices to NASA networks or systems, deeming them "unauthorized devices." In response, NASA employees and partners told the Office of the Chief Information Officer (OCIO) that the policy negatively affected productivity. This feedback contributed to the CIO decision to issue a memorandum in October 2018 that established new requirements allowing NASA employee and partner personally-owned mobile devices (collectively referred to in our report as "non-NASA" IT devices) to securely access the Agency's enterprise email system if the user installed security software known as a Mobile Device Management (MDM) application.

We conducted this audit to assess the Agency's policy and practices regarding the use of non-NASA devices to conduct Agency business. Specifically, we evaluated whether NASA (1) addressed challenges related to non-NASA IT devices gaining unauthorized access to its networks and systems; (2) adequately monitored connection of authorized mobile devices to its enterprise email system; and (3) adequately implemented policy and procedures for non-NASA IT devices accessing NASA networks and systems. To conduct our work, we interviewed officials across NASA, reviewed and analyzed OCIO documentation, reviewed personnel usage and system services to understand access issues related to non-NASA IT devices, reviewed the Agency's efforts to secure its networks and systems from unauthorized IT devices, and assessed overall compliance with NASA's mobile device management requirements.

## WHAT WE FOUND

NASA is not adequately securing its networks from unauthorized access by IT devices. Although OCIO has deployed technologies to monitor unauthorized IT device connections, it has not fully implemented controls to remove or block these devices from accessing NASA's networks and systems. The initial December 2019 target date for NASA to complete installation of these controls has been delayed due to technological challenges and changes in OCIO mission priorities and requirements. Until the enforcement controls are fully implemented, NASA remains vulnerable to cybersecurity attacks.

While OCIO established a process to implement MDM on personal mobile devices, it is not adequately monitoring and enforcing the business rules necessary for granting such access. For example, NASA does not adequately assess whether users accessing its email system have a business need to use a personal mobile device or if the mobile device is ineligible for participation in the MDM service because it violates supply chain controls—all of which increases the risk of the device being exploited. This is because OCIO did not establish monitoring and enforcement requirements when planning the MDM project. As a result, NASA data is at risk from the use of unauthorized devices, which could expose the Agency to viruses, malware, or hacking.

Further, while NASA has improved its overall IT security posture in recent years, we found OCIO's visibility into IT authorization practices at its numerous Centers and facilities around the country remains limited. Although the NASA CIO is responsible for developing, documenting, and implementing the Agency-wide information security program, OCIO relies on Center-based CIOs and staff to implement and enforce the Agency's information security policies. This practice has allowed Centers to tailor processes to meet their own priorities, which has in turn led to inconsistent implementation of NASA's enterprise-wide IT security management. Such a decentralized approach to cybersecurity management limits OCIO's ability to effectively oversee NASA's information security activities and make informed decisions related to project timelines, costs, and efficiencies. It also jeopardizes the success of OCIO's efforts to mitigate the risk of unauthorized devices accessing NASA's networks.

## WHAT WE RECOMMENDED

To improve NASA's management of non-NASA IT device access to Agency networks and systems, we recommended that the Acting Chief Information Officer:

1. Fully implement Network Access Control and Continuous Diagnostics and Mitigation at all Centers to detect, prevent, and remove unauthorized IT devices accessing NASA networks.
2. Incorporate into applicable IT policy and requirements documents IT systems security controls for life cycle management in accordance with National Institute of Standards and Technology Special Publication 800-124.
3. Define requirements and implement controls to monitor and enforce MDM business rules, including defining the office responsible for performing monitoring and enforcement.
4. Revise cybersecurity policy, guidance, and requirements to provide OCIO with a level of direct oversight of enterprise-wide IT management to ensure consistent practices across Centers.
5. Revise the NASA Strategy to Improve Network Security to implement controls to ensure adequate Senior Agency Information Security Officer visibility into cybersecurity practices at the Centers.

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

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

# TABLE OF CONTENTS

# Acronyms

| | |
|---|---|
| ATO | Authorization to Operate |
| CDM | Continuous Diagnostics and Mitigation |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CSPD | Cybersecurity and Privacy Division |
| DEFEND | Dynamic and Evolving Federal Enterprise Network Defense |
| DHS | Department of Homeland Security |
| FISMA | Federal Information Security Modernization Act |
| FY | fiscal year |
| GAO | Government Accountability Office |
| IT | information technology |
| MDM | Mobile Device Management |
| NAC | Network Access Control |
| NAMS | NASA Access Management System |
| NIST | National Institute of Standards and Technology |
| NPD | NASA Policy Directive |
| NPR | NASA Procedural Requirements |
| NSINS | NASA Strategy to Improve Network Security |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| RISCS | Risk Information Security Compliance System |
| SAISO | Senior Agency Information Security Officer |
| VPN | Virtual Private Network |

# INTRODUCTION

Smartphones and tablets (collectively referred to as mobile devices in this report) and laptop computers are integral to the work of NASA employees and their contractor, academic, federal, and international partners (partners). However, use of this equipment to access NASA non-public networks and systems increases opportunities for individuals and organizations to improperly access Agency data. Although NASA does not generally permit personally-owned mobile devices and laptop computers to access Agency networks and systems, authorized mobile devices and users are allowed to access NASA's enterprise email system if they adhere to specified business rules.[1] Additionally, based on the terms of their respective agreements with NASA, partners may be allowed to use partner-owned computers to access the Agency's enterprise and mission networks and systems.

Many types of information technology (IT) equipment, including mobile devices and laptop computers, are available commercially, and in an increasingly interconnected society the lines between personal and corporate devices can become blurred.[2] Because NASA allowed employees and partners to use their own IT devices to access email and other NASA systems, the Agency faced multiple network and system risks. These risks include IT devices that contain unknown applications or those that communicate over untrusted networks.

For years, NASA had permitted personally-owned and partner-owned IT devices to access non-public data through Agency networks and systems, even if those devices did not have a valid authorization. In April 2018, the Agency's Chief Information Officer (CIO) issued a policy memorandum clarifying existing NASA requirements to disallow connection of personally-owned and partner-owned IT devices to NASA networks or systems, deeming them "unauthorized devices." The CIO defined an unauthorized IT device as any electronic equipment that:

- connects to NASA's internal or non-public network and
- does not have an approved Authorization to Operate (ATO) from a NASA Authorizing Official.[3]

In response to the April 2018 memorandum, NASA employees and partners told the Office of the Chief Information Officer (OCIO) that the policy to prohibit the use of non-NASA devices to access email and other NASA applications negatively affected their productivity. This matter contributed to the CIO issuing a follow-up memorandum in October 2018 establishing new requirements that allowed NASA employee and partner (non-NASA) personally-owned mobile devices to connect securely to the Agency's enterprise email system if the user installed security software, a Mobile Device Management (MDM) application.

---

[1] The enterprise email system is used Agency-wide to meet common needs for email versus other systems used in particular parts of the organization for specific mission purposes.

[2] NASA defines IT devices as laptops, smartphones, desktops, tablets, servers, storage devices, and cellphones.

[3] An Authorizing Official is a senior official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations. An ATO is an Authorizing Official's formal acceptance that the security of an information system's operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system's confidentiality, integrity, and availability.

Since November 2006, we have consistently considered NASA's efforts to address its long-standing IT governance and security concerns as a top management challenge.[4] Accordingly, we conducted this audit to assess the Agency's policy and practices regarding the use of non-NASA devices to conduct Agency business. Specifically, we evaluated whether NASA (1) addressed challenges related to non-NASA IT devices gaining unauthorized access to its networks and systems; (2) adequately monitors connection of authorized mobile devices to its enterprise email system; and (3) adequately implemented policy and procedures for non-NASA IT devices accessing NASA networks and systems.

# Background

## Federal Cybersecurity Guidance

The Federal Information Security Modernization Act (FISMA) of 2014 requires federal agencies to guard against unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.[5] A May 2017 Executive Order requires federal agencies to (1) have a cybersecurity risk management process that aligns with strategic, operational, and budgetary planning processes and (2) use the National Institute of Standards and Technology (NIST) standard, *The Framework for Improving Critical Infrastructure Cybersecurity* to manage cybersecurity risk.[6]

Further, Office of Management and Budget (OMB) requirements and NIST guidance call for federal agencies, as part of their information security programs, to authorize the operation of information systems, which include IT devices, and explicitly accept any associated risks to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of an agreed-on set of security controls.

## Office of the Chief Information Officer

NASA's OCIO is responsible for the Agency's IT governance and compliance with reporting, managing, and securing the Agency's enterprise IT assets and operations (see Figure 1 for the OCIO organizational structure).[7] Authority for developing IT policies and implementing Agency-wide IT programs lies with the Headquarters-based Agency CIO. In addition to the Headquarters-based Agency CIO, each NASA Center has a CIO while each Mission Directorate has an IT official with the duties of a CIO. The Agency CIO is responsible for providing leadership, planning, policy direction, and oversight of Agency-wide IT resources. The Agency CIO also serves as the principal advisor to the NASA Administrator and other senior officials on IT matters and is responsible for ensuring NASA acquires and manages its information assets in accordance with federal requirements.

---

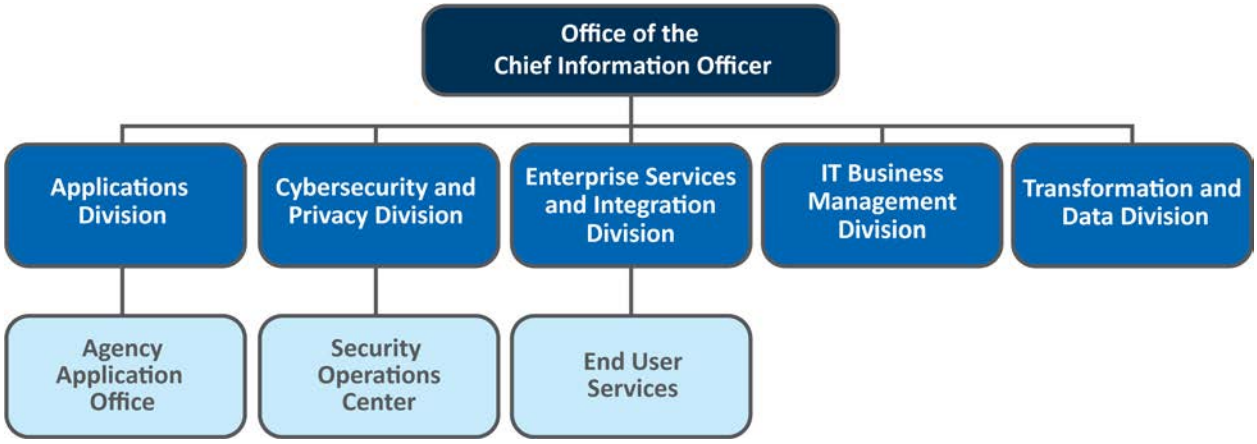
[4] NASA Office of Inspector General (OIG), *NASA's Most Serious Management and Performance Challenges* (November 9, 2006). All of the OIG's Top Management and Performance Challenges reports are located at https://oig.nasa.gov/challenges.html (accessed June 12, 2020).

[5] 44 U.S.C. § 3554.

[6] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017) and NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018).

[7] NASA consists of a Headquarters office in Washington, D.C.; nine geographically dispersed Centers; the Jet Propulsion Laboratory, a federally funded research and development center operated under contract by the California Institute of Technology; and nine component facilities and testing sites such as the Katherine Johnson Independent Verification and Validation Facility and the White Sands Test Facility. For readability, in this report we refer to Headquarters as a Center. See Appendix A for the Centers contacted during this audit.

**Figure 1: Office of the Chief Information Officer as of May 2020**




Source: NASA OIG presentation of Agency data.

NASA's CIO is mandated under federal requirements to appoint a Senior Agency Information Security Officer (SAISO). The SAISO is responsible for NASA's information security program, including: adopting new information security technologies throughout the Agency; establishing a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA's information security program; and ensuring NASA develops, disseminates, annually reviews, and appropriately updates policy, procedure, and technical documentation related to information security.

The SAISO also oversees the Cybersecurity and Privacy Division (CSPD) which manages the Agency-wide information and cybersecurity program to correct known vulnerabilities, reduce barriers to cross-Center collaboration, and provide cost-effective cybersecurity services in support of NASA's information systems, including IT devices. The SAISO works to ensure that cybersecurity across NASA meets confidentiality, integrity, and availability objectives for data and information systems, to include disaster recovery and continuity of operations for critical systems. CSPD maintains a cybersecurity program that ensures consistent security policy, identifies and implements risk-based security controls, and tracks security metrics to gauge compliance and effectiveness. CSPD also manages the NASA Security Operations Center (located at Ames Research Center in Mountain View, California, and at Johnson Space Center in Houston, Texas) which provides 24-hour incident response and manages the Agency's IT threat assessment and incident management programs.

The Enterprise Services and Integration Division manages the portfolios for all enterprise IT services and is responsible for the Agency-wide information management framework and NASA's enterprise architecture. Within this Division, the End User Services Office provides computer hardware, software, and help-desk service to NASA employees and partners. Specific services supported by this office include enterprise e-mail, laptop and desktop computers, mobile devices, and other end-user support capabilities.

The Applications Division manages the planning, design, integration, and delivery of NASA's enterprise applications projects and services. The Agency Application Office is responsible for developing plans and projects supporting the use of IT devices to access NASA's network and applications.

# IT Devices Used to Access NASA Networks

Tens of thousands of IT devices owned by NASA, its partners, and employees access Agency networks and systems each day. As shown in Table 1, these devices fall into four general categories based on ownership and management.

**Table 1: Category and Number of IT Devices Based on Management and Ownership (as of May 2020)**

| Type of IT Device | IT Device Description | Number of IT Devices Connecting to NASA Networks |
|---|---|---|
| *NASA enterprise-furnished devices* | NASA acquires IT devices and services from its enterprise-wide support service contractor to access enterprise and mission networks and systems.[a] | 53,839 |
| *Other NASA-furnished devices* | Individual NASA offices purchase IT devices and obtain associated data services outside of the Agency's enterprise-wide support service contract to access enterprise and mission networks and systems. | 18,207 |
| *Partner devices* | NASA's partners own the IT devices, which are allowed to access NASA's enterprise and mission network and systems. | Unknown[b] |
| *Personal mobile devices* | An employee or partner personally owns and pays for the smartphone, tablet, and associated data charges and is allowed access to NASA's enterprise email system. | 1,293[c] |

Source: NASA.

[a] NASA pays the support service contractor monthly for the devices and associated services (e.g., data charges).

[b] According to OCIO, there currently is no authoritative source to obtain the number of partner-owned IT devices accessing NASA networks and systems.

[c] Only includes personally-owned mobile devices accessing NASA's Office 365 enterprise email system.

# NASA Policies for Accessing Networks and Systems

Since 2006, NASA policy specifically prohibits unauthorized IT devices from accessing its networks and systems; however, this policy was not routinely enforced.[8] Through the years, OCIO has issued updated guidance and policy related to the use of personally-owned mobile devices. In August 2013, the NASA CIO issued a memorandum, "Minimum Security Requirements for Personal Mobile Devices," alerting employees that it planned to enforce several security requirements for users of NASA's email system beginning in September 2013 such as requiring at least a four-character password on mobile devices and automatic locking after a period of inactivity. These policies were released in parallel with NASA's expanded telework program that provided eligible employees the opportunity to work from anywhere.[9]

[8] NASA Policy Directive (NPD) 2810.1A, *NASA Security of Information Technology* (May 16, 2006) requires that NASA information and information systems be protected from unauthorized disclosure, destruction, or modification.

[9] NASA Shared Services Center, NSEN-3000-0079, *Work From Anywhere - NASA's Telework Program* (March 2013).

OCIO also planned to develop a policy to govern the use of personally-owned IT devices to conduct Agency business which it planned to present to stakeholders by mid-February 2014. However, due to changes in OCIO leadership priorities and the complexity of creating enterprise-wide networks and processes with Centers that have historically operated decentralized networks and systems, that policy was never finalized.

In 2015, the CIO issued the *Center Bring Your Own Device Wireless Infrastructure Standard*, which allowed credentialed employee and partner personally-owned mobile devices to access the Agency enterprise systems, including email and other applications such as NASA's time and attendance and travel systems.[10] OCIO established several controls to protect the Agency networks and systems in addition to reminding employees to be vigilant when using mobile devices to access its networks and systems. For example, in August 2017 OCIO instituted security requirements including passwords, inactivity locking, password failure lock, and encryption which added controls to secure systems from unauthorized access.

In April 2018, the NASA CIO issued a memorandum clarifying that the use of any unauthorized IT device, including personal devices, to access NASA networks and systems was not permitted under Agency policy.[11] The CIO issued another memorandum in October 2018 establishing rules for using NASA employee and partner (non-NASA) personally-owned mobile devices to connect to the Agency's enterprise e-mail system.

## Past NASA Practices for Accessing Networks and Systems

Protecting sensitive data is a complex task that involves managing encryption technologies, commercial security patching, personal data, privacy issues, and addressing lost or stolen devices. At NASA, these standard risks associated with IT devices were heightened by a number of vulnerabilities including:

- Many of NASA's IT systems were directly accessible from any IT device using simple password authentication, making NASA systems and data easy targets for attackers.
- NASA employees and partners connected to the internal Agency network with personally-owned computers and mobile devices that may have been infected with malware, compromised by hackers, or used by other family members, exposing NASA systems to vulnerabilities and access by unauthorized individuals.
- Partners used company computers to access the internal NASA network without appropriate limitations on what they could access, potentially allowing unauthorized access to systems and data.
- When mobile devices, personal computers, and partner systems connected to the internal NASA network, there were no checks to prevent unauthorized uploading and downloading data or to ensure basic security configurations.

[10] NASA-STD 2850.7, (April 9, 2015).

[11] NASA CIO's Memorandum, *Use of Unauthorized Devices* (April 16, 2018).

# NASA's Strategy to Improve Network Security

To better secure NASA's networks, systems, and data, OCIO is leading the Agency-wide IT initiative known as NASA Strategy to Improve Network Security (NSINS). NSINS is built around seven targets: (1) modernize networks, (2) simplify and secure access to IT systems/data, (3) ensure only authorized IT devices are connected, (4) promote and enable secure collaboration, (5) secure mobile access to NASA systems/data, (6) secure software use, and (7) address and develop cybersecurity integration and resources. These targets were developed to describe the projects and initiatives required to secure NASA data, with Target 3 focusing on unauthorized IT devices and Target 5 on mobile devices. Before initiating NSINS, OCIO needed to develop a series of foundational technical and hardware elements that include the NASA network (both internal and external), a multi-factor authentication mechanism (a trusted way to collaborate with partners), and a method to permit only authorized IT devices access to the NASA internal network.[12] OCIO launched NSINS in April 2018 and expects to substantially complete the initiative in fiscal year (FY) 2022. Figure 2 (next page) depicts the seven NSINS targets and their associated projects.

Since beginning this strategy in 2018, NASA has implemented numerous controls for IT infrastructure and enhanced capabilities under Targets 1 through 5 that have improved access security for mobile devices and computers, including laptops. Specifically,

- External Border Protection Enforcement of Trusted Internet Connection Firewalls (Target 1.2)—provides the foundation for secure collaboration via an enterprise Virtual Private Network (VPN) as well as a method for enforcing firewalls and trusted internet connections to provide consistent protection borders for all Centers.[13] This control has been implemented at all Centers and allows laptop computers to remotely access NASA's internal networks with proper authorization.
- Unauthorized Device Phase 1 (Target 3)—provides authorized IT devices access to NASA enterprise email system (Microsoft Office 365). Unauthorized Phase 1 also implemented certificate-based authentication for Microsoft Office 365 services, which closed a significant security challenge from the previous NASA email system.
- Microsoft Office 365 (Target 4.1)—provides secure cloud storage for NASA email, calendar, and contacts as well as other NASA data.
- Mobile Device Management (MDM) (Target 5.1 and 5.2)—provides management and secure, encrypted access of NASA employee and partner personally-owned mobile devices to NASA's Office 365 email system.

[12] Multi-factor authentication is an authentication method in which an IT device user is granted access only after successfully presenting two or more pieces of evidence, such as a password, smart card or a fingerprint to an authentication mechanism. This evidence must come from two different categories to enhance security, i.e., entering two different passwords would not be considered multi-factor.

[13] Trusted internet connection is an OMB-mandated initiative to enhance network security across the federal government through consolidating external connections and deploying common tools at internet access points. VPN is built on top of existing networks to provide a secure communications mechanism for data and Internet Protocol information transmitted between networks.

**Figure 2: NASA Strategy to Improve Network Security**


Source: NASA OIG presentation of NASA information.
Note: NAC is Network Access Control, and PIV is Personal Identity Verification.

# NASA Mobile Device Management

To address the issues identified by the NASA Office of Inspector General (OIG) concerning the lack of sufficient security controls for personal devices accessing NASA networks and systems, OCIO began planning for the MDM project in 2013, which included a two-phased approach as shown in Table 2. MDM provides enhanced data protection on mobile devices through data encryption, deployment of mobile applications, and asset tracking and management. MDM software is installed on NASA-issued mobile devices as well as NASA employee and partner personally-owned mobile devices, making a portion of the device (a container) authorized to connect to specific NASA networks and systems. Any data stored in the MDM container is segregated from other data on the mobile device. The data within the MDM container is NASA property and the container can be deleted from the mobile device remotely if warranted.

**Table 2: Mobile Device Management Phases**

| MDM Phases | Task | Project Period |
|---|---|---|
| MDM Phase 1 | Plan, test, and implement MDM Project: Provide a mobile device registration process and install MDM software on NASA support service contractor furnished mobile devices. | June 2013 to September 2015 |
| MDM Phase 2 | Enhance MDM capabilities: Make MDM software available for NASA employee and partner personally-owned mobile devices and implementing additional controls to secure NASA data such as stronger credential and authentication management, encrypted email, and container to access NASA email. | October 2015 to October 2018 |

Source: NASA.

OCIO selected IBM's MaaS360 software as its MDM software and purchased it through an IT support service contractor for NASA enterprise-issued mobile devices. In October 2015, OCIO began implementing MDM on NASA enterprise-issued mobile devices in a phased deployment to the Centers, and then in October 2018 expanded the MDM capabilities and installation to other mobile devices owned by NASA, partners, and employees.

# NASA's Networks and Systems Are Not Adequately Secured Against Access from Unauthorized IT Devices

NASA is not adequately securing its networks from unauthorized access by IT devices (smartphones, tablets, and laptop computers). Although OCIO has implemented technologies to monitor unauthorized IT device connections, it has not fully implemented enforcement controls to remove or block unauthorized IT devices from accessing NASA's networks and systems. The initial December 2019 target date for NASA to complete installing these controls has been delayed. The OCIO has not been able to fully implement these enforcement controls on the scheduled timetable due to technological challenges and changes in OCIO mission priorities and requirements. Consequently, NASA remains vulnerable to cybersecurity attacks because enforcement controls to block unauthorized IT devices from accessing its networks and systems are not fully in place and operational.

## OCIO Has Not Fully Implemented Enforcement Controls to Secure Networks and Systems

NASA is monitoring its enterprise networks and systems for connection of unauthorized IT devices, and the Agency is able to detect when such connections occur. However, OCIO has yet to enable the enforcement of security controls to actually block unauthorized IT devices from accessing its network because OCIO has not fully implemented Network Access Control (NAC), which is a component of Continuous Diagnostics and Mitigation (CDM). NAC is a tool for controlling access to the wired network, to the wireless network, and to VPN. It ensures that all connected devices are automatically identified, classified, authorized, and given policy-based access control. NAC is part of the Department of Homeland Security's (DHS) CDM Program.[14] The CDM Program delivers capabilities in five key areas—dashboard, access management, identity and access management, network security management, and data protection management.[15]

Once fully implemented, NAC and CDM will give NASA the ability to block access from unauthorized devices across its enterprise networks. Specifically, NAC will enable NASA to implement policies for controlling devices and user access to their enterprise networks. If a device attempts to make a connection, NAC will use an identity and access management program to check users for appropriate permissions based on NAC policies established by OCIO. When fully implemented, NAC will provide

[14] CDM is coordinated by DHS to support all civilian sector federal departments and agencies. CDM provides federal agencies with capabilities and tools that find cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, enable cybersecurity personnel to focus on the most significant problems immediately, and streamline FISMA reporting.

[15] NAC is part of CDM network security management capability, also known as the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND).

NASA the ability to deny enterprise network access to unauthorized devices, place devices in an isolated area of the network if suspected of having a virus, or provide devices limited access.

CDM should provide NASA the capabilities to identify cybersecurity risks on an ongoing basis and prioritize those risks based on potential impacts. CDM will conduct cybersecurity assessments and expand the Agency's continuous diagnostic capabilities by increasing the capacity of its network sensors, automating data collection from sensors, and prioritizing risk alerts. The CDM Program offers a catalog of commercial off-the-shelf tools—including NAC, which NASA began implementing in January 2017.[16]

NASA is moving towards checking every IT device that attempts to access its networks and systems to ensure it is authorized. As a part of NSINS, OCIO developed a three-phased implementation plan to identify unauthorized IT devices, summarized in Table 3, to monitor and block such devices from accessing Agency networks and systems, a plan that aligns with Target 3 of NSINS. As of June 2020, OCIO has completed Phase 1—Foundation, and is currently implementing Phase 2—Transition. OCIO plans on completing Phase 3—Enforcement—by the end of 2022. However, before this can be accomplished NASA must fully implement NAC and CDM; modernize its networks for wired and wireless IT devices, access control, and zoning; and enhance and enforce its network firewalls, web content filters, and VPN.

According to OCIO officials, once all phases of the plan are implemented, OCIO anticipates blocking 80 percent of all unauthorized IT devices from accessing NASA's networks and systems. To address the remaining 20 percent—which will be related to issues with the Agency's Mission networks—OCIO intends to (1) convert partner-owned devices to authorized IT devices by establishing approved IT system security plans; (2) provide approval from an Authorizing Official for the use of IT devices accessing the networks and systems; and (3) continuously assess risks as new security requirements develop.[17]

[16] According to OCIO officials, NASA is working directly with DHS and is on schedule with CDM DEFEND for implementing NAC at NASA.

[17] According to OCIO officials, Mission networks are not controlled by OCIO.

**Table 3: Unauthorized IT Device Implementation Plan**

| Phase | Task | Start date | Estimated completion date | Factors impacting whether milestone is achieved |
|---|---|---|---|---|
| Phase 1: Foundation | Implemented infrastructure to enable technical security access controls<br>• *NAC/Network Zones*<br>• *VPN/Remote Access*<br>Implemented email enterprise system<br>• *MDM/Personal Device Access*<br>• *Office 365 Controls to safeguard against unauthorized access* | November 2018 | Completed January 2020 | N/A |
| Phase 2: Transition | Authorize partner devices both onsite and for remote uses when solutions are ready<br>• *NAC/Network Zones*<br>• *VPN/Remote Access*<br>Implement/Assess risk based decision where standard solutions do not fit<br>Implement solutions and enforce compliance based on Centers' Transition Plans | In progress | December 2020 | Coordinate with Centers to obtain transition plans for NAC enforcement<br>Continue to build partner network zones for federal, international, and other partners<br>Full implementation of NAC and CDM |
| Phase 3: Enforcement | Enforce access control compliance<br>Complete Risk Based Decision Plan of Action and Milestones where required[a] | In progress | December 2022 | Full implementation of NSINS Targets 1, 2, and 3 |

Source: NASA.

[a] When OCIO is working to certify a partner IT device, security plan, or software an official plan is created to define the actions and milestones needed.

## Current State of Enforcement Controls Being Implemented

NAC is enabled and functional, but NASA needs to fully implement its ability to block unauthorized IT devices from accessing networks and systems. OCIO has limited implementation of NAC to NASA enterprise and Agency-managed infrastructure networks (i.e., partner networks) but not the Mission networks.[18] NAC has two modes—monitoring and enforcement. As of March 2020, NASA has NAC enforcement on its wireless networks at all Centers and had begun enforcing NAC controls on its wired networks.[19]

OCIO is using NAC's monitoring mode to authenticate IT devices on its systems and to report devices that cannot be authenticated. OCIO plans to have the enforcement mode operational and 80 percent compliant with FISMA requirements by December 2020.[20] OCIO officials explained that an 80 percent

[18] OCIO has not deployed an enterprise NAC solution on its Mission networks. On March 3, 2020, NASA made the decision to extend the Agency's NAC solution to the Mission networks.

[19] According to OCIO officials, as of January 2020 the NAC infrastructure was 64 percent implemented and NAC blocked 40 percent of the unauthorized devices.

[20] OCIO's April 2018 policy memorandum clarified that unauthorized devices are not permitted to connect to any network or system that processes NASA non-public data.

compliance goal may be challenging to meet at Centers that have partners using internal networks. Partner access to Agency internal networks leaves NASA more vulnerable because the partners' systems are not managed or monitored by the Agency. OCIO is working to develop networks for partner use based on their IT device trust and authorization requirements, which NASA will need to establish before NAC can be fully enforced. OCIO cannot fully implement NAC enforcement mode until they can account for every IT device that attempts to access a particular network and understand how the device will be authenticated. According to OCIO officials, full implementation of NAC enforcement must consider continuity across Centers, ensure operational consistency, and identify potential impacts on partners.

OCIO has taken steps to implement NAC enforcement by testing its VPN capabilities to ensure unauthorized IT devices, such as laptop computers, are not accessing NASA's networks. VPN is an encrypted connection over the internet that prevents unauthorized IT devices from accessing a network. Therefore, through VPN technology, OCIO has been able to check whether an IT device meets NASA's established security requirements before it is allowed to connect remotely.

As of June 2020, OCIO has conducted assessments on the Agency VPN system at four Centers—Glenn Research Center, Langley Research Center, Marshall Space Flight Center, and Stennis Space Center. Under the assessment, any users from those Centers who log onto the VPN system would be permitted access only if their IT device is authorized. OCIO is working to implement the posture assessment for VPN at the remaining Centers but must do so one Center at a time to ensure missions are not negatively impacted. Overall, OCIO is working to move all Centers to using NAC for VPN access, but for now is focused on getting all Centers to use CDM to control VPN access. OCIO has taken steps to fully enforce NAC and CDM through its unauthorized IT device implementation plan.

OCIO is continuing to work with DHS to implement CDM for cybersecurity tools, integration services, and dashboards through four security enhancement phases to improve NASA's security posture and help better manage IT devices. These phases include identifying users and IT devices on the network, describing what is happening on the network, and defining how data is being protected. OCIO has deployed tools for network vulnerability scanning to identify devices on the network, which is critical to IT device management. OCIO has also implemented tools to identify users on the network by establishing identity and credential management (i.e., identity verification and personal identity verification cards), as well as expanded integration where passwords will be eliminated for users to access the networks.

## Challenges with Implementing Enforcement Controls

OCIO has delayed the expected implementation plan completion date several times from the initial December 2019 target date. OCIO has not been able to fully implement enforcement controls due to technological challenges and changes in mission priorities and requirements. Specifically, OCIO has faced challenges in obtaining authentication certificates for certain IT devices.[21] For example, OCIO manages enterprise IT contracts and is able to install certifications on IT devices that are provided under those contracts. However, they are unable to install certificates on IT devices that fall under Center or Mission Directorate contracts because those devices must be certified by those entities. Also, according to OCIO, it lost 2 months of productivity due to the government shutdown in 2019, which required OCIO

[21] Certificate authentication is the use of a digital certificate (credential) to verify that a device connected to an organization's network is authorized.

to restart NAC testing for Windows, Mac, and Linux machines.[22] This delayed certificate deployments on IT devices, which in turn delayed NAC enforcement activities.

In addition, OCIO has experienced challenges ensuring partners are able to meet mission requirements while adopting enhanced IT security measures, a situation that creates additional complexities in moving towards having a fully functional enterprise system security. For example, NASA must ensure partners have access to both NASA mission networks and their own corporate networks without compromising the security of either network. Consequently, OCIO will have to work through these issues before it can approve partner security plans and develop the partner networks. According to officials, addressing these issues will take time and one reason OCIO has not implemented full NAC enforcement.

Furthermore, OCIO said providing support for NASA's Mission Support Future Architecture Program and the Artemis mission has impeded its efforts to implement NAC and CDM.[23] Under the Mission Support Future Architectural Program, all mission support services including OCIO will move to an enterprise operating model. Therefore, OCIO—in addition to its regular duties—is evaluating service functions at all levels through working groups, which is a time-consuming process. OCIO also has staff within the Artemis program whose sole responsibility is to provide direct cyber support to Artemis' Center and Agency-level program offices. This responsibility requires resources and has required OCIO to reprioritize existing work in order to have staff available to work on Artemis requirements.

Lastly, on-site work restrictions associated with the Agency's response to the COVID-19 pandemic have negatively impacted the implementation schedule for NAC and CDM. Specifically, NAC network configurations are on hold at many Centers until normal operations resume and enforcement activities have been limited due to the risk of end users experiencing connectivity issues both remotely and upon return to their Center. Regarding CDM, procurements, system upgrades, and needed enhancements have been delayed, and hands-on work in laboratories has been postponed. As of May 2020, OCIO was working with DHS to revise plans and schedules for CDM implementation.

## NASA Networks at Risk until NAC and CDM Are Fully Implemented

Until NASA fully implements NAC and CDM enforcement controls, the Agency cannot ensure that only authorized IT devices are accessing its enterprise and mission networks and systems. In addition, NASA's ability to effectively monitor, detect, report, and respond to security incidents is hindered by not having a fully implemented network access enforcement solution. Unauthorized IT devices connecting to NASA's networks and systems can expose sensitive data such as intellectual property and personally identifiable information, as well as provide access to critical NASA assets. Importantly, access by unauthorized IT devices often leads to data loss and malware, malicious attacks, security breaches, and data spills.[24] For example, NASA disclosed a data breach in October 2018 during which an unknown intruder gained access to one of its servers that stored personal data of current and former employees. In another instance in 2019, a NASA contract employee used a personal computer to access NASA-owned networks and systems to mine cryptocurrency.

[22] MDM addresses mobile device operating systems.

[23] In 2017, NASA initiated the Mission Support Future Architecture Program to optimize procurement and other services by moving toward a more interdependent model that enables the Agency to share capabilities across Centers, realign budget structure, and improve procurement services through collaboration. With the Artemis program, NASA plans to land astronauts on the Moon by 2024.

[24] The National Security Agency defines data spill as the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications, or media.

# NASA Is Not Fully Enforcing Mobile Device Management Rules

Even though OCIO established a process to implement MDM on mobile devices that access NASA's enterprise email system, it is not adequately monitoring and enforcing the business rules established for mobile devices. For example, NASA does not adequately assess whether users accessing its email system have a business need to use a personal mobile device or if the mobile device is ineligible for participation in the MDM service because it violates supply chain controls, increasing the risk of the device being exploited. This is because OCIO did not establish monitoring and enforcement requirements when planning the MDM project. As a result, NASA data is at risk from the use of unauthorized devices, which could hinder the Agency's efforts to secure its information and email system from being compromised by viruses, malware, or hacking.

## Allowing Mobile Devices to Connect to NASA Networks and Systems

OCIO's April 2018 policy memorandum resulted in personal and partner IT devices not being allowed to access any NASA enterprise network and system. Employee dissatisfaction with this lack of access contributed to OCIO issuing a follow-up policy memorandum in October 2018 to allow limited use of NASA employee and partner personally-owned mobile devices to connect only to the NASA email, calendar, and contacts system. OCIO now requires MDM—which safeguards NASA data on the mobile device—to be installed on any mobile device that connects to the enterprise email system.[25] To obtain MDM, users need to have either NASA personal identity verification privileges or a NASA smart badge. In addition, users are required to have an approved business need to access email. Users are eligible to enroll their personal mobile device in MDM if they meet baseline requirements and accept NASA's User Agreement.

## NASA Established Mobile Device Management Controls but Several Are Not Enforced

As previously described, OCIO implemented MDM over several years, including establishing a formal user agreement, instructions, and information.[26] Additionally, OCIO created requirements, known as business rules, tailored to NASA's MDM process and effectively communicated the process to Centers

[25] As of March 2020, NASA's enterprise email system is the only Agency enterprise network or system that uses the MDM software on mobile devices. Using the NAC infrastructure, OCIO plans to implement MDM or a similar control to protect NASA data and allow mobile devices to connect to other Agency approved services.

[26] *Government Furnished Equipment and Personal Device Business Rules for Enrollment in NASA's Mobile Device Management Service* (November 5, 2018), *NASA Mobile Device Management Personal Device Annual User Agreement and Authorization, Mobile Device Management MaaS360 User Guide* (version 1.3, September 6, 2018), *Mobile Management Device Frequently Asked Questions* (version 3, April 11, 2019), and *Things You Need to Know* (version 2, March 1, 2019).

and users through presentations, publications, and a website.[27] However, as shown in Table 4, OCIO is not enforcing all established business rules for mobile devices.[28]

**Table 4: Enforcement of MDM Business Rules for Mobile Devices**

| MDM Business Rule | Enforcement Control | Adequate Control Enforced |
|---|---|---|
| Users should not enroll any non-NASA provided or personal mobile device in MDM until they have been migrated to Office 365 email system. | OCIO Requirement | Yes |
| Users registering a personal mobile device will be required to submit a NASA Access Management System (NAMS) approval request.[a] | NASA Access Management System | Yes |
| All users registering a personal mobile device will be required to accept the MDM User Agreement and Authorization terms of use via NASA online training. | NASA Access Management System | Yes |
| Users who have an enrolled NASA furnished mobile device are not eligible to enroll a personal mobile device in MDM service. | NASA Access Management System | Yes |
| Users are only allowed to enroll one personal mobile device in MDM service. | NASA Access Management System | Yes |
| A mobile device can only accommodate one MDM service. | MDM software | Yes |
| Users of personal devices must accept the MDM user agreement annually to continue using the MDM. | NASA Access Management System | Yes |
| Users must remain up to date on the operating system for the mobile device. | MDM software | Yes |
| Civil Servant, contractor personnel, and partners must require remote access to NASA email, calendaring, and/or contacts to effectively perform NASA duties. | NASA supervisor and Center OCIO authorizing official | No |
| Some mobile devices are not eligible for participation in the MDM service because they violate supply chain controls. | None | No |
| NASA and partner personnel who have the MDM service installed on their personally-owned mobile device shall not access the MDM service from their device while outside the United States and its territories. | NASA Procedural Requirements | No |

Source: NASA OIG analysis of Agency data.

[a] NAMS is the Agency's centralized system for requesting and maintaining accounts for NASA's physical and logical systems and applications and a repository of user account information, access requests, and account maintenance processes for NASA employees, contractors, and remote users.

[27] We determined OCIO has 11 MDM business rules that were enforceable.

[28] We did not evaluate the NASA Access Management System (NAMS) or MDM systems or test and evaluate the effectiveness of the information system's controls.

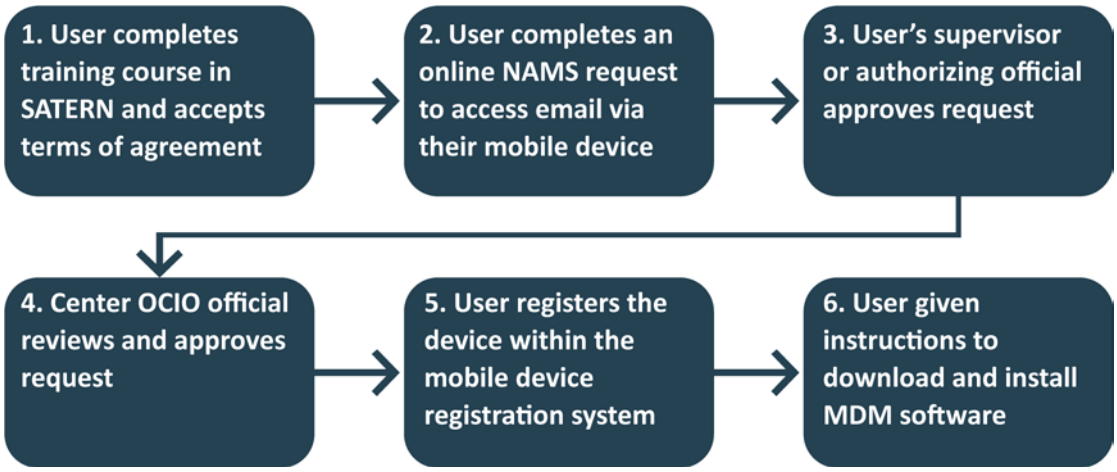
## NASA Instituted Effective Controls for Some MDM Processes and Business Rules

In November 2018, OCIO established business rules for government-issued mobile devices, as well as NASA employee and partner personally-owned mobile devices enrolled in NASA's MDM service. As of June 2020, OCIO was enforcing 8 of the 11 business rules through a NASA system or MDM software. However, OCIO only recently began enforcing one of these business rules.

In May 2020, OCIO began taking action to uninstall MDM on mobile devices with outdated operating systems, which will terminate the user's access to NASA's email system. Prior to this, the user suffered no consequence for failing to update a government issued or NASA employee or partner personally-owned mobile device's operating system in a timely manner, even though the user would have received five notifications to update the device's operating system. Without an up-to-date version of an operating system, mobile devices can be exploited and then potentially used to exfiltrate information from the NASA email system. As of March 2020, OCIO reported 1,470 mobile devices had outdated operating systems—1,316 government and 154 personal mobile devices. Additionally, OCIO identified 151 registered Apple mobile devices (111 government and 40 personal) that were unable to update the operating system due to the device's age and limited capabilities; therefore, the MDM container will be uninstalled on those devices and the user's access to NASA email system via the mobile device will be terminated unless the user updates the device's operating system. We remain concerned about the implementation of this new control until we validate its reliability.

OCIO established a formal process for a user who voluntarily requests installation of MDM on their personal mobile device, as shown in Figure 3.

**Figure 3: NAMS User Workflow Request for MDM Installation**




Source: NASA OIG presentation of Agency data.

Note: SATERN (System for Administration, Training, and Educational Resources for NASA) is NASA's online training system.

OCIO instituted the following controls as part of the MDM installation process:

- NAMS has an automated control that will not allow a request if the training was not completed.
- The supervisor's signature in NAMS, "…authorizes that the requestor has a legitimate requirement for access to NASA email from their personal [mobile] device."
- If the user's NAMS request is pending or disapproved, the MDM registration system will not allow the user to register their personal mobile device.
- MDM software provides a container on the mobile device that securely separates NASA data from other applications on the device, allowing access to NASA email, calendar, contacts, and internet and preventing data from being downloaded outside the container. MDM and other NASA systems provide an approved user verification, automatic locking the mobile device when not used, password protection, and device configuration restrictions.

We found OCIO has not monitored and enforced the remaining three MDM business rules.

- Legitimate Business Need is Required to Access NASA Email – OCIO is not actively enforcing this rule. NASA OCIO is relying on the supervisor's approval as the sole control to ensure this business rule is achieved. We believe this is an inadequate control because supervisory review may be cursory. Additionally, 9 of the 10 Center OCIO officials stated their Center is not reviewing user's NAMS request to ensure the user requires their personal mobile device to access to the email system to perform their work. Only one Center OCIO official informed us they were periodically monitoring MDM requests through NAMS to ensure that only users with a legitimate reason were approved to use personal mobile device to access NASA email system. Another Center OCIO official informed us of their Center's general policy to not allow personal mobile devices to connect to NASA email.

  Additionally, after MDM is installed on a personally-owned mobile device, OCIO is not monitoring the frequency with which users are accessing their email, which could be an indicator of whether a person has a legitimate and ongoing business need to have MDM on their personal mobile device.

- Mobile Device Supply Chain Controls – Certain types of mobile devices are not eligible for participation in NASA's MDM software because they violate federal supply chain controls, increasing the risk of the device being exploited. Federal law prohibits U.S. government agencies from using mobile devices from specific foreign manufacturers and their subsidiaries, namely Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company.[29] Neither NASA's MDM business rules nor other MDM guidance define supply chain controls and risks nor explain what mobile devices violate this policy. Therefore, we question the ability of users and approving officials to meet this business rule absent a more complete explanation. Additionally, we found OCIO is not monitoring or enforcing this business rule.

  Instituting a control regarding prohibited IT devices that should not be permitted to access NASA networks and systems would address supply chain risks associated with IT devices manufactured in China. Federal law defines these risks as adversary sabotaging and maliciously introducing unwanted functions to surveil, deny, disrupt, or otherwise degrade the operation of a system. We identified a lack of communication from OCIO to Center OCIOs regarding supply chain violations and prohibited mobile devices. In March 2019, the Security Operations Center began

[29] Pub. L. No. 115-232, *John S. McCain National Defense Authorization Act for Fiscal Year 2019* (August 13, 2018).

manually checking for prohibited mobile devices quarterly by reviewing the MDM user log.[30] During the first month, the Security Operation Center identified 439 mobile devices that violated the federal supply chain requirement. When a prohibited mobile device is identified, a security incident ticket is created and sent to the user's Center OCIO for resolution. An OCIO official stated this manual review is very time consuming, an ineffective use of resources, and is not performed frequently enough to be effective. According to an OCIO official, CSPD plans for the Security Operations Center to automate this review in the future, which will allow prohibited mobile devices to be identified soon after MDM is loaded onto a device.

We also found the supply chain violations, controls, and risks were not defined and explained in the (1) MDM business rules, (2) MDM guidance to users and centers, (3) online training, or (4) NAMS approval process to install MDM. Therefore, we question whether users are even aware of this business rule let alone able to abide by it.

Additionally, although the user self-certifies in both the training and NAMS systems that there is a business need for using a mobile device, the user does not self-certify that their mobile device does not violate the federal supply chain requirements. This self-certification and the supervisor's approval in NAMS, although not the most effective control, would provide a preliminary control that could be used along with other monitoring and enforcement efforts.

- Accessing NASA Email While Outside the U.S. – In accordance with an MDM business rule, Agency personnel that have NASA MDM installed on their personally-owned mobile device are not permitted to access the MDM service while outside the U.S. and its territories. According to DHS, use of mobile devices outside the U.S. exposes the device to loss, theft, eavesdropping, and other increased vulnerabilities and heightened risks to mobile device security; therefore, controls over mobile devices are needed. However, we found that OCIO is not monitoring or enforcing this business rule.

  OCIO officials told us this rule is being enforced through the revised NASA requirements for the use of NASA information systems outside the U.S.[31] The revised requirement states that (1) international travelers shall only take NASA IT devices or access NASA accounts when authorized by OCIO prior to international travel; and (2) personnel who have the MDM application installed on their personally-owned mobile devices shall not access the application while outside the U.S., unless it necessary to conduct business and prior approval is granted through their Center OCIO. The policy states that users shall not access, from outside the U.S., any NASA systems, networks, or data not intended for access by the public unless these conditions have been met. While the requirements appear sound, we believe the control is not sufficient because NASA does not actively monitor compliance and enforce the business rule.

  NASA has the capability through MDM to track a mobile device anywhere on the globe; however, OCIO has not activated this capability. An OCIO official stated that the MDM feature, known as geofencing, was not implemented because of privacy issues associated with NASA continually tracking a user's location for personally-owned mobile devices. Separate from geofencing, the Security Operations Center monitors all IT devices, including personally-owned mobile devices, that attempt to access NASA networks and systems from foreign countries through the device's internet protocol address. An OCIO official stated this type of tracking is

[30] NASA OIG, *Audit of NASA's Security Operations Center* (IG-18-020, May 23, 2018).

[31] NASA Procedural Requirements (NPR) 2810.2, *Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories* (October 29, 2019).

currently a manual, labor-intensive process and therefore is not regularly performed. Although the CSPD plans for the Security Operations Center to use an automated tool to monitor mobile devices connecting from abroad, as of April 2020 the OCIO had no timetable to implement the tool.

# Lack of Planning and Resources for Monitoring and Enforcing Mobile Devices Rule Increased Risks to NASA

OCIO initially did not monitor and enforce MDM business rules because they were not considered during the development of the MDM project plan. We found that the MDM project plan did not encompass the reporting and monitoring component of the life-cycle process, as required by NASA's IT project management requirements.[32] Additionally, NIST states that security controls should be included as part of the life cycle for MDM.[33] Furthermore, the MDM life cycle includes operations and maintenance phases and security-related tasks an organization should perform regularly, such as:

- Checking for upgrades and patches to the mobile device solution components (including mobile device infrastructure components, mobile device operating systems, and mobile device applications).
- Reconfiguring access control features based on factors such as policy changes, technology changes, audit findings, and new security needs.
- Detecting and documenting anomalies within the mobile device infrastructure through continuous monitoring, including unauthorized configuration changes to mobile devices that might indicate malicious activity.
- Revoking access to or deleting an application that has already been installed but subsequently has been assessed as too risky to use.

According to NIST, organizations should also periodically perform assessments to confirm that the organization's mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

In addition, the MDM compliance rules were not being enforced due to (1) lack of an automated capability to enforce the rule, (2) limited staffing resources, and (3) the amount of time and resources needed to configure system to monitor mobile devices. OCIO does not have an automated capability to monitor MDM logs, and an OCIO official told us that manually reviewing these logs is resource intensive and cost prohibitive. OCIO officials said they are planning to use an existing automated IT tool to periodically review MDM logs; however, implementing this tool for MDM monitoring requires additional funding, and it will be a time-consuming process to establish and expand the database capability.

Without adequate monitoring and enforcement of the MDM controls, NASA data remains at risk from unauthorized devices, which could hinder Agency efforts to secure its information and email system from being compromised by viruses, malware, or hacking. Additionally, malicious applications could

[32] NASA Interim Directive 7120.99, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements* (December 22, 2011); NID 7120.99 remains effective until the revision of NPR 7120.7 version A, which as of May 2020 was in process, is approved.

[33] NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).

take control of mobile devices. OMB reported in 2018 that phishing attacks on email systems is one of the most common attack vectors across both government and industry. Failing to properly secure, monitor, and enforce guidelines on mobile devices accessing NASA's email system represents an avenue to infiltrate the system containing data on Agency missions and sensitive government functions.

# NASA's Decentralized Approach to Cybersecurity Limits OCIO Visibility into Centers' Practices

While NASA has improved its overall IT security posture in recent years, we found OCIO's visibility into IT authorization practices at the Centers remains limited. Although the NASA CIO has the responsibility to develop, document, and implement the Agency-wide information security program, OCIO relies on Center CIOs and staff to implement and enforce the Agency's information security policies—a practice that has allowed Centers to tailor processes to meet their own priorities, which has led to inconsistency in NASA's strategic IT management. This decentralized approach to cybersecurity management limits OCIO's ability to effectively oversee NASA's information security activities and make informed decisions related to project timelines, costs, and efforts to mitigate inefficiencies. It also jeopardizes the success of OCIO's efforts to mitigate the risk of unauthorized access from non-NASA IT devices to Agency networks and systems and renders IT assets vulnerable to cybersecurity attacks.

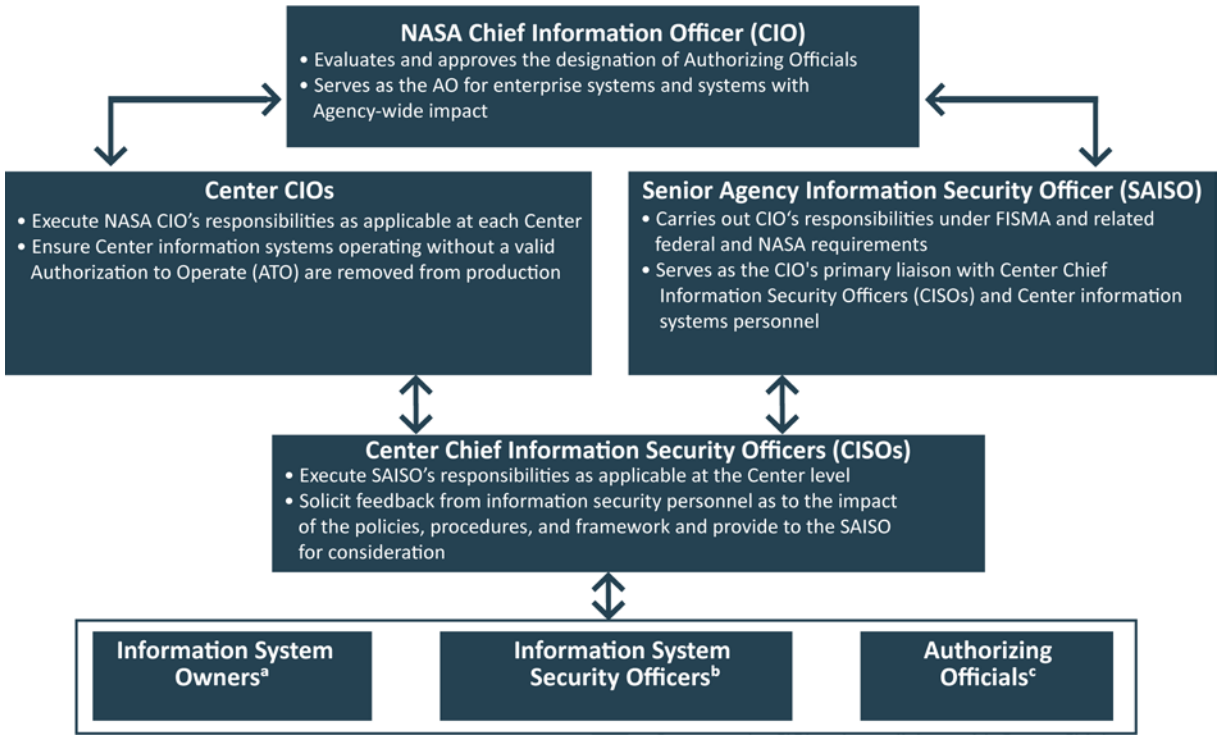
## OCIO's Delegation of Responsibilities

NASA OCIO has no direct control over the implementation and enforcement of cybersecurity operations, including the network and systems access authorization process at Centers. Although the CIO appropriately designated the SAISO to carry out federal and NASA cybersecurity requirements, the SAISO further delegated this responsibility to Center Chief Information Security Officers (CISO). Center CISOs also serve as the primary interface between the SAISO and Center information security functions.[34]

As a result of this layered delegation of authority, the SAISO and OCIO have no direct control over Center-based implementation and enforcement of cybersecurity requirements, which has led to inconsistent application of the authorization process at the Centers. The SAISO and OCIO rely on the Center CISOs to oversee Center information security operations, solicit input from the Centers' information security personnel—such as the Information System Owners, Center Authorization Officers, and Information System Security Officials—and report on the impact of the information security policies, procedures, and framework. Figure 4 depicts this delegation of authority and information flow.

[34] NPR 2810.1A, *Security of Information Technology* (May 16, 2006).

**Figure 4: Delegation of NASA CIO's Information Security Responsibilities**




Source: NASA OIG presentation of Agency information.

[a] Information System Owners ensure information security system security deficiencies and weaknesses are identified, minimized, or eliminated; and provide feedback to Center CISOs and Authorizing Officials regarding the impact of information security requirements on the operation of their information systems.

[b] Information System Security Officers oversee day-to-day security operations of their information system and advise Information System Owners on information security.

[c] Authorizing Officials ensure information systems operate with a valid ATO; approve or revoke information system's ATO; and approve acceptance of risk requests and any changes to the plan of action and milestones.

## Inconsistent Cybersecurity Practices at Centers

OCIO's reliance on Centers to implement Agency IT security policy has led to inconsistent application of the authorization process across NASA. According to OCIO officials, the authorization process for IT systems and devices to access Agency networks at some Centers is unnecessarily complicated and, in some instances, can take 6 months to complete. For example, smaller partners such as academic institutions have complained that the ATO process is too complicated for their short-term projects related to the International Space Station, and that they have been unable to complete the ATO before the work was completed. According to these same officials, the process at other Centers is lax and insufficient to address significant system security risks. OCIO officials provided several reasons for these inconsistencies, such as size and complexity of systems and programs at the different Centers, available IT security resources, and varying degrees of familiarity with the authorization requirements.

OCIO officials told us that some Centers and missions, such as the Huntsville Operations Support Center at Marshall Space Flight Center and the Joint Polar Satellite System at Goddard Space Flight Center, have excelled with the authorization process. These Centers developed Memoranda of Understanding, standardized forms, and checklists to better streamline their processes. However, OCIO officials also acknowledged that, at times, Center-specific approaches created Agency-wide inconsistencies. For

instance, while OCIO requires security control assessments of the Centers' authorization process once every 3 years, it does not enforce how the Centers conduct these assessments. According to OCIO and Center OCIO officials, this could lead to project delays due to resource or skill limitations, and unplanned costs to perform the assessments. Another Center OCIO official stated that because of these inconsistencies, the Center would prefer Agency-wide standards and perhaps the Centers could use Agency-provided services to meet their assessment needs.

Allowing Centers to manage IT security policy without adequate OCIO oversight could also hinder NASA-wide efforts to gauge unauthorized access to Agency networks and systems and render Agency IT assets more vulnerable to cybersecurity attacks. According to a NASA Security Operations Center FY 2019 fourth quarter threat report, 12 NASA Centers and facilities experienced incidents that involved individuals gaining unauthorized access from IT devices to the Agency's non-public networks, systems, and data. This was a 36-percent increase in incidents from the previous quarter and resulted in the loss and exposure of personally identifiable information, International Traffic in Arms Regulations data, Export Administration Regulation data, and sensitive but unclassified data, costing NASA $92,737 to mitigate the damages. Unauthorized access can happen from a variety of sources, including unauthorized mobile devices. The lack of consistent application of security controls to mobile devices likely has contributed to these security incidents.

## Efforts to Improve Visibility of Center IT Security Practices

Recognizing the need to enhance its oversight of Center IT security practices, OCIO has been revising policies and developing a more robust strategy for improving the Agency's overall IT security posture over the past 2 years. For instance, in an effort to improve the Agency authorization process, the CIO issued a memorandum in February 2019 assuming responsibility for the designation and performance evaluation of Authorizing Officials for all NASA information systems that process NASA data and operate within the Agency's environment. The memorandum not only reaffirmed the CIO's responsibilities as the Authorizing Official for enterprise systems and systems with NASA-wide impact, but also added a requirement that for other information systems, Mission Directorate Deputy Associate Administrators, Deputy Center Directors, Centers CIOs, or other cognizant senior NASA officials may be designated to serve as Authorizing Officials. Prior to this policy change, lower-level officials at the Centers could be Authorizing Officials, so this change elevated accountability for the IT security authorization process.

The CIO serves as the Authorizing Official for enterprise systems and systems with NASA-wide impact—approximately 9 percent of all NASA systems—which causes additional process delays due to extra layers of review needed prior to the CIO's signoff. OCIO officials from several Centers stated that following the February 2019 memorandum, the ATO review process has not improved, and has caused further process delays. An OCIO official confirmed these delays and acknowledged that the changes following the memorandum only partially improved CIO visibility into NASA information systems and the ATO process. For example, The Boeing Company (Boeing) has ATOs at multiple Centers; however, Boeing experienced delays and inefficient implementation due to differing requirements resulting from the inconsistent authorization processes at the Centers. An OCIO official noted that they are working to improve this by creating an enterprise ATO with Interconnection Security Agreements to connect systems. This would not only improve overall CIO visibility, but would also better secure NASA information and information systems from partner IT devices by ensuring consistent processes. Until then, the lack of adequate CIO visibility into Center IT security practices and delays in approving ATOs could potentially allow IT devices and systems to operate within NASA networks with unmitigated security deficiencies, which poses increased security risks to the Agency.

NASA's Risk Information Security Compliance System (RISCS) could provide a means for enabling better OCIO decisions on mitigating IT risk and ensuring a consistent assessment and authorization processes and practices.[35] However, as we previously reported, Center IT security personnel do not promptly and accurately update system security information in RISCS.[36] As a result, OCIO cannot rely on RISCS to monitor and assess the cybersecurity posture of NASA IT assets and make well-informed decisions affecting the Agency's overall information security posture. Moreover, even if RISCS is fully utilized, OCIO would be unaware of irregularities in the authorization process because it lacks direct oversight. OCIO is working on improvements to automate some of the processes within RISCS for better record keeping, as well as making enhancements, per NIST 800-171, for more consistency in data entry into RISCS.

As previously discussed, NASA's Strategy to Improve Network Security (NSINS) is supporting OCIO's effort to move toward Agency-wide management of IT security. NASA's unauthorized IT device policy reinforcing the Agency authorization requirements for non-NASA IT devices is a part of the NSINS strategy. However, the current strategic planning to improve the management and security of non-NASA IT devices does not include mechanisms for addressing the need for enhanced OCIO visibility into the authorization process. An OCIO official agreed on the significance of incorporating better visibility into the overall IT strategy and said including this as an action item within NSINS could be beneficial.

Policy changes, such as reinforcing the Agency authorization requirements for non-NASA IT devices and enhancing the selection process for Center AOs, are important steps toward strengthening OCIO's visibility into Center cybersecurity practices. However, further improvements are needed to ensure that Center IT security processes are efficient and consistently applied throughout the Agency. Without proper oversight and enforcement, OCIO will not be able to make informed decisions on mitigating IT risk or accurately assess the effectiveness of the Agency's cybersecurity posture. Furthermore, Centers will continue to make program and mission-specific decisions tailored to meet their priorities, which may not address Agency-wide challenges.

[35] RISCS is NASA's centralized toolset that integrates data sources to provide a holistic, risk-based view of NASA's IT systems and operating environment.

[36] NASA OIG, *Review of NASA's Information Security Program under the Federal Information Security Modernization for Fiscal Year 2018 Evaluation* (ML-19-002, March 6, 2019).

# CONCLUSION

For years, NASA allowed personally-owned and partner-owned IT devices to access Agency networks and systems with minimal controls in place to safeguard NASA assets. In 2018, NASA's OCIO clarified the Agency's policy to prohibit unauthorized IT devices from connecting to its non-public networks and systems and established requirements under which NASA employee and partner personally-owned mobile devices could access the Agency enterprise e-mail system. Since then, OCIO has implemented technologies to monitor unauthorized IT device connections but has not fully implemented enforcement tools to block unauthorized devices from accessing NASA's networks and systems. While OCIO is working to fully implement enforcement tools, the target date for completion has slipped several times. Until these efforts are completed, NASA cannot adequately secure its networks from unauthorized IT device access and will be vulnerable to cybersecurity attacks.

For IT security to work effectively, approved mobile devices must be monitored and established business rules need to be enforced. NASA must also retain high levels of control over access to its systems. To this end, all mobile devices that connect to NASA email are required to have MDM installed. However, OCIO is not adequately monitoring and enforcing MDM's business rules and controls, potentially exposing NASA's email system and data to viruses, malware, or hacking through connected mobile devices.

Overall, NASA has improved its IT security posture in recent years but OCIO's visibility into IT authorization practices at the Centers remains limited. The Agency's decentralized approach to cybersecurity management limits OCIO's ability to effectively oversee Centers' information security activities and make informed, enterprise-wide decisions. It also jeopardizes the success of OCIO's efforts to mitigate the risk of unauthorized access to Agency networks and systems and renders Agency IT assets vulnerable to cybersecurity attacks. We acknowledge the inherent difficulty in balancing Center-specific flexibilities and desire for autonomy with the need for a robust, enterprise-wide approach to IT security. However, in the face of persistent cybersecurity threats, NASA needs to quickly move to a more consistent, enterprise-wide approach to identifying and managing these risks.

# RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To improve NASA's management of non-NASA IT device access to Agency networks and systems, we recommended that the Acting Chief Information Officer:

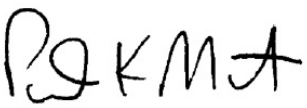
1. Fully implement NAC and CDM at all Centers to detect, prevent, and remove unauthorized IT devices accessing NASA networks.
2. Incorporate into applicable IT policy and requirements documents IT systems security controls for life cycle management in accordance with NIST Special Publication 800-124.
3. Define requirements and implement controls to monitor and enforce MDM business rules, including defining the office responsible for performing monitoring and enforcement.
4. Revise cybersecurity policy, guidance, and requirements to provide OCIO with a level of direct oversight of enterprise-wide IT management to ensure consistent practices across Centers.
5. Revise NSINS to implement controls to ensure adequate SAISO visibility into cybersecurity practices at the Centers.

We provided a draft of this report to NASA management, who concurred with all of our recommendations. We consider management's comments responsive; therefore, the recommendations are resolved and will be closed upon verification and completion of the proposed corrective actions. Management's comments are reproduced in Appendix B. Technical comments provided by management and revisions to address information the Agency identified that should not be publicly released have been incorporated as appropriate.

---

Major contributors to this report include Raymond Tolomeo, Science and Aeronautics Director; Adrian Dupree, Project Manager; David Lu, Sashka Mannion, Jobenia Parker, Matt Ward, and Lynette Westfall.

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.



Paul K. Martin
Inspector General

# APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from March 2019 through July 2020 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.

Our overall objective was to evaluate NASA's policy and practices regarding the use of non-NASA smartphones, tablets, and laptop computers to conduct Agency business. Specifically, we evaluated whether NASA (1) addressed challenges related to non-NASA IT devices gaining unauthorized access to its networks and systems; (2) adequately monitored connection of authorized mobile devices to its enterprise email system; and (3) adequately implemented policy and procedures for non-NASA IT devices accessing NASA networks and systems.

To determine if NASA has addressed challenges related IT devices gaining unauthorized access to its networks and systems, we conducted interviews with OCIO Headquarters officials to gain and understanding of what technologies NASA is using to monitor and detect unauthorized IT device connections. We reviewed and analyzed OCIO decision briefs, updates, and memorandums pertaining to unauthorized IT device use including OICO's three-phased implementation plan as well as information pertaining to NAC and CDM enforcement tools designed to block unauthorized access to Agency networks and systems. We also reviewed use cases from NASA Centers that identified Agency network and system technical and access issues related to non-NASA IT devices.

To evaluate how NASA is monitoring the connection of authorized non-NASA mobile devices to the Agency's enterprise email system, we interviewed OCIO Headquarters officials to gain an understanding of the MDM process, including monitoring and enforcing MDM controls and business rules. We reviewed and analyzed various MDM documents including MDM's Project Plan, registration and approval guidance, and MDM briefings to the CIO. We also reviewed the NAMS user request workflow information for MDM installation and *NASA's Cybersecurity and Privacy Rules of IT Behavior* for mobile device use. We obtained reports from the MDM registration system and cybersecurity incident reports for government and personnel mobile devices from OCIO's Security Operation Center. We obtained information on Center operations through a questionnaire and interviews.

To determine whether NASA implemented policy and procedures for non-NASA IT devices accessing NASA networks and systems, we conducted interviews with OCIO Headquarters and officials from Ames Research Center, Armstrong Flight Research Center, Glenn Research Center, Goddard Space Flight Center, Johnson Space Center, Kennedy Space Center, Langley Research Center, Marshall Space Flight Center, and Stennis Space Center to gain an understanding of NASA current policy and procedures it has for network and system access for non-NASA IT devices including its ATO process. We reviewed and analyzed NSINS initiatives aimed at assisting the Agency in moving toward Agency-wide management of Agency IT security activities. We also reviewed documents in NASA's RISCS including the MDM package and security plan as well as NASA's delegation of authority for its cybersecurity operations. In addition, we sent a 14-question email survey to all 10 Center OCIOs and collected responses from each regarding how Center OCIO officials were implementing policy and practices related NSINS.

To gain an understanding of NASA's policy and practices with the use of non-NASA IT devices to access the Agency's networks and systems, we conducted our review at NASA Headquarters. We also obtained and examined internal and external applicable documents related to the use of non-NASA IT devices. The documents we examined included the following:

Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017)

44 U.S. Code § 3554, *Federal Information Security Modernization Act of 2014* (December 18, 2014)

NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013)

NPD 2540, *Personal Use of Government Office Equipment Including Information Technology* February 24, 2016 and *Acceptable Use of Government Office Property Including Information Technology* (August 19, 2019)

NPD 2810.1E, *NASA Information Security Policy* (July 14, 2015)

NASA Interim Directive (NID) 7120.99, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements* (December 22, 2011)

NPR 2810.2, *Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories* (October 29, 2019)

NASA Technical Standard 2850.7, *Center Bring Your Own Device Wireless Infrastructure Standard*

OCIO Policy Memorandum, *Use of Personally-Owned Mobile Devices to Connect to NASA Email, Calendar and Contact Services* (October 25, 2018)

OCIO Policy Memorandum, *Use of Unauthorized Devices* (April 16, 2018)

OCIO *Security Policies on Handheld Devices* (August 23, 2017)

## Assessment of Data Reliability

The computer processed data used in this audit did not materially affect the findings; therefore, we did not test the reliability and validity of the data.

## Review of Internal Controls

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. We reviewed and evaluated internal controls related to the use of non-NASA IT devices connecting to NASA's networks and systems. This included reviewing NASA efforts with securing its networks and systems from unauthorized IT devices. We also assessed compliance with NASA's mobile device management business rules, guidelines, and a user manual for mobile devices that connect to the Agency-wide email system. We concluded that there are opportunities for NASA to (1) improve its internal controls regarding unauthorized IT devices accessing its networks and systems and (2) monitor and enforce established rules for mobile devices connecting to NASA's enterprise email. The internal control recommendations discussed in the report, if implemented, should correct the weaknesses identified. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

# Prior Coverage

During the last 7 years, the NASA OIG and U.S. Government Accountability Office (GAO) issued 15 reports of significant relevance to the subject of this report. These reports can be accessed at http://oig.nasa.gov/audits/reports and https://www.gao.gov.

# NASA Office of Inspector General

*NASA's Top Management and Performance Challenges* (November 13, 2019)

*Cybersecurity Management and Oversight at the Jet Propulsion Laboratory* (IG-19-022, June 18, 2019)

*NASA's Information Security Program under the Federal Information Security Modernization for Fiscal year 2018 Evaluation* (ML-19-002, March 6, 2019)

*Audit of NASA's Security Operations Center* (IG-18-020, May 23, 2018)

*Final Memorandum, Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation* (IG-18-003, A-17-004-00, November 6, 2017)

*NASA's Efforts to Improve the Agency's Information Technology Governance* (IG-18-002, October 19, 2017)

*Industrial Control System Security Within NASA's Critical and Supporting Infrastructure* (IG-17-011, February 8, 2017)

*Report Mandated by the Cybersecurity Act of 2015* (IG-16-026, July 27, 2016)

*NASA's Management of its Smartphones, Tablets, and Other Mobile Devices* (IG-14-015, February 27, 2014)

# U.S. Government Accountability Office

*Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices* (GAO-19-545, July 2019)

*Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (GAO-18-93, August 2018)

*NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses* (GAO-18-337, May 2018)

*Federal Chief Information Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority* (GAO-16-686, August 2016)

*Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services* (GAO-15-431, May 2015)

*Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* (GAO-12-757, September 2012)

# APPENDIX B: MANAGEMENT'S COMMENTS

National Aeronautics and
Space Administration

**Headquarters**
Washington, DC 20546-0001


August 20, 2020

Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Acting Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, "Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices" (A-19-010-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices" (A-19-010-00), dated July 27, 2020.

In the draft report, the OIG makes five recommendations addressed to the Acting Chief Information Officer (CIO) intended to improve NASA's management of non-NASA information technology (IT) device access to Agency networks and systems.

Specifically, the OIG recommends the following:

**Recommendation 1:** Fully implement network access control (NAC) and continuous diagnostics and mitigation (CDM) at all Centers to detect, prevent, and remove unauthorized IT devices accessing NASA networks.

**Management's Response:** Concur. NASA will continue to implement the NASA strategy to improve network security (NSINS) started in 2018 to deploy NAC. NASA continues to work with the Department of Homeland Security's Continuous Diagnostics and Mitigation Dynamic and Evolving Federal Enterprise Network Defense (DHS CDM DEFEND) program to fully implement NAC at all Centers to detect, prevent, and remove unauthorized IT devices accessing NASA corporate networks.

**Estimated Completion Date:** September 30, 2021.

**Recommendation 2:** Incorporate into applicable IT policy and requirements documents IT systems security controls for life cycle management in accordance with NIST Special Publication 800-124.

**Management's Response:** Concur. NASA will incorporate appropriate requirements into applicable IT policy and requirements documents for managing security of mobile devices in accordance with the National Institute of Standards and Technology Special Publication 800-124.

**Estimated Completion Date:** December 15, 2021.

**Recommendation 3:** Define requirements and implement controls to monitor and enforce the mobile device management (MDM) business rules, including defining the office responsible for performing monitoring and enforcement.

**Management's Response:** Concur. NASA will define requirements and implement controls to monitor and enforce the MDM business rules, including defining the office responsible for performing monitoring and enforcement.

**Estimated Completion Date:** December 15, 2021.

**Recommendation 4:** Revise cybersecurity policy, guidance, and requirements to provide OCIO with a level of direct oversight of enterprise-wide IT management to ensure consistent practices across Centers.

**Management's Response:** Concur. As part of the NASA's Mission Support Future Architecture Program (MAP), OCIO's MAP activities will yield many positive results that will improve OCIO's oversight of enterprise-wide IT management to ensure consistent practices across Centers and OCIO. OCIO will also revise cybersecurity policy, guidance, and requirements accordingly to reflect future mission support architecture.

**Estimated Completion Date:** December 15, 2021.

**Recommendation 5:** Revise NASA strategy to improve network security (NSINS) to implement controls to ensure adequate Senior Agency Information Security Officer (SAISO) visibility into the cybersecurity practices at the Centers.

**Management's Response:** Concur. Building upon response to Recommendation #4, the OCIO will revise cybersecurity policy, guidance, and requirements accordingly to include refining the Cybersecurity Program Service Office focus and augmented via an enterprise contract for cybersecurity services across all NASA Centers, including

mission IT support. NSINS Target States and/or Objectives will be revised to track these change(s) and efforts.

**Estimated Completion Date:** December 15, 2021.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have identified some 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 Fatima Johnson on (202) 358-1631.

JEFFREY SEATON Digitally signed by JEFFREY SEATON
Date: 2020.08.20 15:31:09 -04'00'

Jeff Seaton

# APPENDIX C: REPORT DISTRIBUTION

*National Aeronautics and Space Administration*

Administrator
Deputy Administrator
Associate Administrator
Deputy Associate Administrator
Chief of Staff
Chief Information Officer

*Non-NASA Organizations and Individuals*

Office of Management and Budget
    Deputy Associate Director, Energy and Space Programs Division

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

*Congressional Committees and Subcommittees, Chairman and Ranking Member*

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

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

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 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-19-010-00)**