

NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

NASA'S CYBERSECURITY READINESS

May 18, 2021

Report No. IG-21-019





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

NASA's Cybersecurity Readiness

May 18, 2021

IG-21-019 (A-20-009-00)

WHY WE PERFORMED THIS AUDIT

Given its high-profile mission and broad connectivity with the public, educational institutions, and outside research facilities, NASA presents cybercriminals a larger potential target than most government agencies. The Agency's vast online presence of approximately 3,000 websites and more than 42,000 publicly accessible datasets also makes it highly vulnerable to intrusions. In recent years, NASA has worked to improve its cybersecurity readiness with efforts led by the Office of the Chief Information Officer (OCIO). Nonetheless, in the last 4 years alone NASA experienced more than 6,000 cyber-attacks, including phishing scams and introduction of malware into Agency systems. Consequently, it is vital that the Agency develop strong cybersecurity practices to protect itself from current and future threats.

NASA's information technology (IT) assets generally fall into two broad categories: institutional and mission systems. Three primary levels of management oversee these assets and are responsible for cybersecurity management. OCIO personnel oversee the institutional and security capabilities that support the entire NASA workforce. Missions typically fund their own networks and their IT personnel have visibility over the operational and security aspects of these networks.

Finally, IT personnel at NASA Centers manage and oversee operations for programs and projects located there, which includes both institutional and mission networks.

NASA's IT assets generally fall into two broad categories:

Institutional systems...

support the day-to-day work of NASA employees...

and include networks, data centers, web services, and desktop and laptop computers.



Mission systems...

support the Agency's aeronautics, science, and space exploration programs...

and host IT systems that control spacecraft and process scientific data.

To assess NASA's cybersecurity readiness, we examined whether: (1) the OCIO enterprise architecture is designed to appropriately assess cybersecurity risks and threats; (2) NASA's cybersecurity protection strategy is risk-based; (3) cybersecurity resource allocations are adequate and appropriately prioritized; and (4) Agency cybersecurity risks are effectively assessed using sound IT security practices.

To complete this work, we reviewed applicable laws and regulations, interviewed OCIO personnel, reviewed Agency documentation, analyzed budgeting and staffing data, and reviewed past cyber breaches. We relied for guidance on the National Institutes of Standards and Technology (NIST) Cybersecurity Framework and 800 Series Special Publications, the Center for Internet Security Top 20 Controls, and the Federal Enterprise Architecture.

WHAT WE FOUND

Attacks on NASA networks are not a new phenomenon, although attempts to steal critical information are increasing in both complexity and severity. As attackers become more aggressive, organized, and sophisticated, managing and

mitigating cybersecurity risk is critical to protecting NASA's vast network of IT systems from malicious attacks or breaches that can seriously inhibit the Agency's ability to carry out its mission. Although NASA has taken positive steps to address cybersecurity in the areas of network monitoring, identity management, and updating its IT Strategic Plan, it continues to face challenges in strengthening foundational cybersecurity efforts.

We found that NASA's ability to prevent, detect, and mitigate cyber-attacks is limited by a disorganized approach to Enterprise Architecture. Enterprise Architecture (EA) and Enterprise Security Architecture (ESA)—the blueprints for how an organization analyzes and operates its IT and cybersecurity—are crucial components for effective IT management. Enterprise Architecture has been in development at NASA for more than a decade yet remains incomplete while the manner in which the Agency manages IT investments and operations remains varied and ad hoc. Unfortunately, a fragmented approach to IT, with numerous separate lines of authority, has long been a defining feature of the environment in which cybersecurity decisions are made at the Agency. The result is an overall cybersecurity posture that exposes NASA to a higher-than-necessary risk from cyber threats.

We also noted that NASA conducts its assessment and authorization (A&A) of IT systems inconsistently and ineffectively, with the quality and cost of the assessments varying widely across the Agency. These inconsistencies can be tied directly to NASA's decentralized approach to cybersecurity. NASA plans to enter into a new Cybersecurity and Privacy Enterprise Solutions and Services (CyPrESS) contract intended to eliminate duplicative cyber services, which could provide the Agency a vehicle to reset the A&A process to more effectively secure its IT systems.

WHAT WE RECOMMENDED

In order to strengthen NASA's cybersecurity readiness and provide process continuity and improved security posture for NASA's systems, we recommended the Associate Administrator and the Chief Information Officer:

1. Integrate EA and ESA, and develop metrics to track the overall progress and effectiveness of EA.
2. Collaborate with the Chief Engineer on strategies to identify and strengthen EA gaps across mission and institutional IT boundaries.
3. Evaluate the optimal organizational placement of the Enterprise Architect and Enterprise Security Architect during and after MAP implementation to improve cybersecurity readiness.
4. Determine each Center's annual cost for performing independent assessments, including staffing, during the A&A process for NASA's 526 systems.
5. Develop baseline requirements in the planned CyPrESS contract for a dedicated enterprise team to manage and perform the assessment process for all NASA systems subject to A&A.

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

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

TABLE OF CONTENTS

Introduction.....	1
Background	1
Effectiveness of NASA’s Cybersecurity Efforts Limited by a Disorganized Approach to Enterprise Architecture	10
NASA’s Assessment and Authorization Process Remains Inconsistent and Ineffective	15
Conclusion	20
Recommendations, Management’s Response, and Our Evaluation	21
Appendix A: Scope and Methodology	22
Appendix B: Security Control Ratings	26
Appendix C: Common Attack Vectors.....	28
Appendix D: Management’s Comments.....	29
Appendix E: Report Distribution	32

Acronyms

A&A	Assessment and Authorization
CIO	Chief Information Officer
CSPD	Cybersecurity & Privacy Division
CyPrESS	Cybersecurity and Privacy Enterprise Solutions and Services
EA	Enterprise Architecture
ESA	Enterprise Security Architecture
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
JPL	Jet Propulsion Laboratory
MAP	Mission Support Future Architecture Program
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center

INTRODUCTION

The cyber threat landscape is highly dynamic and extremely difficult to keep pace with. Attackers are not only developing new techniques to evade security, but threats—such as spam, phishing, and malware—are growing in complexity and precision. The importance of having a robust defense against such attacks was highlighted by the SolarWinds breach, a large-scale hack of government and private information technology (IT) assets that became public in December 2020.¹ Meanwhile, IT applications and architecture continue to evolve rapidly during a period of increasing reliance on digital connections during the COVID-19 pandemic.

Given its high-profile mission and broad connectivity with the public, educational institutions, research facilities, and other outside organizations, NASA presents cybercriminals a larger potential target than most government agencies. In response, the Agency has worked to improve its cybersecurity preparedness with efforts led by the Office of the Chief Information Officer (OCIO). Nonetheless, in the last 4 years alone NASA experienced more than 6,000 cyber-attacks, including phishing scams and introduction of malware into Agency systems.² Consequently, it is vital that the Agency develop strong cybersecurity practices to protect itself from current and future threats.

To assess NASA's readiness to identify cybersecurity threats and defend against major cybersecurity breaches, we examined whether: (1) the OCIO enterprise architecture is designed to appropriately assess cybersecurity risks and threats; (2) NASA's cybersecurity protection strategy is risk-based; (3) cybersecurity resource allocations are adequate and appropriately prioritized; and (4) Agency cybersecurity risks are effectively assessed using sound IT security practices. See Appendix A for details of the audit's scope and methodology.

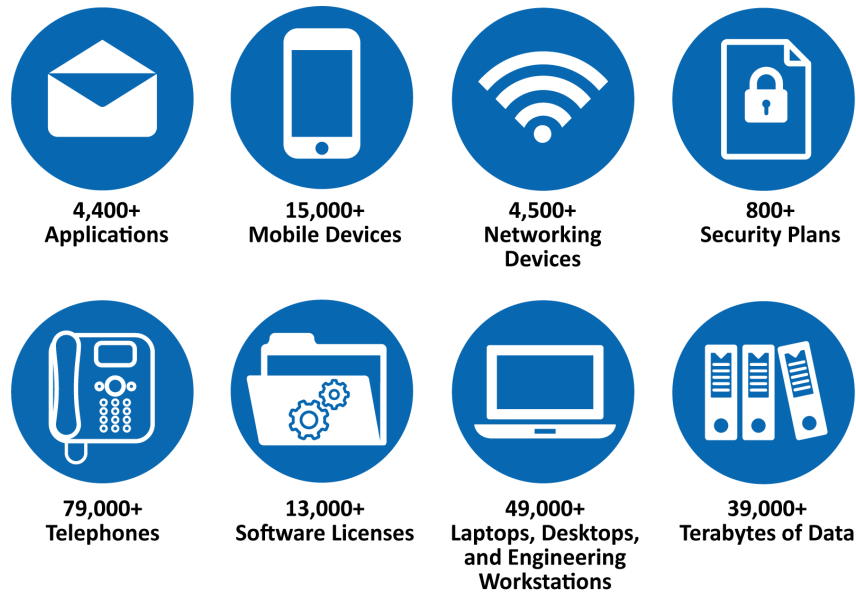
Background

NASA is a regular target of cyber-attacks due in part to its high-profile missions, the sizeable public-facing digital footprint, and the often sensitive nature of the information these systems manage. Given its online presence of approximately 3,000 websites and more than 42,000 publicly accessible datasets, the Agency is highly vulnerable to intrusions. This year in particular NASA has experienced an uptick in cyber threats: phishing attempts have doubled and malware attacks have increased exponentially during the COVID-19 pandemic and the concomitant move to telework for much of the NASA workforce. The Agency's cybersecurity challenges are further exacerbated by the number and variety of IT devices at NASA and the sheer volume of data the Agency maintains, as illustrated in Figure 1.

¹ Hackers, believed to be operating on behalf of a foreign government, breached software provider SolarWinds and deployed a malware-laced update to infect the networks of multiple U.S. companies and government networks. While the investigation is still ongoing, the Cybersecurity and Infrastructure Security Agency (CISA) directed all federal civilian agencies to review their networks for indicators of a compromise and disconnect SolarWinds products immediately. NASA complied with this directive in December 2020.

² A cyber-attack is the targeting of a computing environment/infrastructure for the purpose of disrupting, disabling, or maliciously destroying the integrity of the data or stealing controlled information through attacks such as spam, phishing, and malware. See Table 1 for a more detailed description of cyber-attacks at NASA.

Figure 1: NASA IT by the Numbers



Source: Office of Inspector General (OIG) representation of NASA data.

Cyber incidents at NASA can affect national security, intellectual property, and individuals whose data could be lost or compromised. In cybersecurity, an attack vector is a path or means by which an attacker gains unauthorized access to a computer or network, for example, through email, websites, or external/removable media. Once an attacker gains access, they can exploit system vulnerabilities, gain access to sensitive data, install different types of malware, and launch cyber-attacks. A hack at NASA's Jet Propulsion Laboratory (JPL) in 2018, for example, resulted from an account belonging to an external user connecting an unauthorized device to JPL servers that inadvertently exposed the network to hackers, who then infiltrated the system and accessed the servers as well as NASA's Deep Space Network array of telescopes.³ Further explanation of common attack vectors can be found in Appendix C.

According to NASA data, the Agency identified 1,785 cyber incidents in 2020, as shown in Table 1.⁴ Significantly, improper use incidents—which result from a violation of an organization's acceptable use policies, such as installing unapproved software or viewing inappropriate material—increased the most, from 249 in 2017 to 1,103 in 2020, a 343 percent growth. Further, improper use continued to be the top attack vector type in 2020. NASA officials explained that while the increases are concerning, they believe recently installed cybersecurity software has improved network visibility and contributed to the higher number of recorded incidents.

³ NASA has a contract with the California Institute of Technology (Caltech), a private nonprofit research university, to operate JPL in Pasadena, California, as a federally funded research and development center. Operated by JPL, the Deep Space Network, or DSN, provides deep space missions with the tracking, telemetry, and command services required to control and maintain spacecraft and transmit science data. Although DSN primarily services NASA missions, it also supports missions by NASA's international partners.

⁴ Legacy data has been adjusted to reflect changes to current Federal Information Security Modernization Act reporting parameters.

Table 1: Types of Cyber-Attacks at NASA

Attack Type	FY17	FY18	FY19	FY20
Attrition (<i>brute force network attack</i>)	9	10	0	2
Email	149	97	510	110
External/Removable Media	6	0	6	30
Impersonation (<i>appearing to be from a trusted source</i>)	0	1	0	4
Improper Usage	249	267	805	1,103
Loss/Theft of Equipment	430	392	346	274
Web	391	287	95	219
Other	50	83	126	43
TOTAL	1,284	1,137	1,888	1,785

Source: OIG presentation of NASA data.

Note: FY = fiscal year

The cyber threat to NASA’s computer networks from internet-based intrusions is expanding in scope and frequency, and the success of these intrusions demonstrates the increasingly complex nature of cybersecurity challenges facing the Agency. Simply put, to date the Agency’s IT security processes too often have been ineffective in staying ahead of the dynamic threat landscape. Some key examples of past NASA cyber breaches include:

- In 2019, a NASA contract employee used a personal computer to access NASA-owned networks and systems to mine cryptocurrency.⁵
- In 2019, two Chinese nationals, members of a hacking group operating in China, were indicted on criminal charges for gaining unauthorized access to a NASA computer to steal data.
- In 2018, an account belonging to an external user was compromised and used to steal approximately 500 megabytes of data from a major mission system.

Effective cybersecurity demands focus and dedication, and accurately assessing threats and identifying vulnerabilities is critical to understanding an organization’s risk. As an IT management approach, *cyber risk* combines the probability of a threat with the potential monetary or reputation loss the threat would cause if carried out. In order to understand such risk, it is imperative to accurately assess threats and vulnerabilities. More broadly, cybersecurity is as an important component of the overall risk management process with its success ultimately measured by how well it prevents malevolent attack and intrusion.⁶

⁵ At its simplest, cryptocurrency is a medium of exchange that is digital, encrypted, and decentralized. Unlike the U.S. dollar or the Euro, there is no central authority that manages the value of a cryptocurrency. Instead, these tasks are broadly distributed among a cryptocurrency’s users via the internet. While multiple cryptocurrencies are in circulation worldwide, the most famous is Bitcoin.

⁶ Common security issues include patch management, password control, and system configuration.

Ongoing Cybersecurity Concerns

For almost 20 years we have identified securing NASA's IT systems and data as a top management challenge. Collectively, the OIG and Government Accountability Office (GAO) have issued dozens of reports during the past 5 years identifying weaknesses in NASA's information technology systems. Among the significant findings:

- The Chief Information Officer (CIO) has struggled to implement an effective IT governance structure that aligns authority and responsibility with the Agency's overall mission.
- NASA lacked an Agency-wide risk management framework for information security and an information security architecture.
- Pervasive weaknesses exist in NASA IT internal controls and risk management practices.
- The Security Operations Center lacks visibility and authority to manage information security incident detection and remediation for the entirety of NASA's IT infrastructure.
- NASA's cybersecurity program remained ineffective at a Level 2 out of 5 (Federal Information Security Modernization Act rating)—meaning the Agency has issued, but has not consistently implemented, policy and procedures defining its security program.
- NASA is not adequately monitoring and enforcing the business rules necessary for granting Mobile Device Management access to its network.

Of the 73 IT-related recommendations made by the OIG in the last 5 years, 46 have been closed with appropriate implementation action taken. NASA continues to work toward implementing the remaining 27 recommendations, most of which stem from our more recent work. In addition, during the past 5 years, NASA OIG investigators conducted more than 120 investigations involving intrusions, malware, denial of service attacks, and data breaches on NASA networks, several of which resulted in criminal convictions.

Federal and NASA Cybersecurity Guidance

The National Institute of Standards and Technology (NIST) has issued a suite of information security standards and guidelines for managing cybersecurity risk. In addition, several federal laws and policies establish requirements for protecting federal systems and managing cybersecurity risk. For example, as mandated by the Federal Information Security Modernization Act of 2014 and specified by the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and NIST, cybersecurity programs at federal agencies must provide information security for the IT systems that support the operations and assets of the agency. Federal agencies' cybersecurity programs must also include cybersecurity risk assessments; policies and procedures that reduce information security risks and ensure compliance with all applicable requirements; and security operations such as vulnerability mitigation and incident management.

In this audit, we examined NASA's approach to two of the cornerstones of IT management: Enterprise Architecture (EA) and Enterprise Security Architecture (ESA). EA is a blueprint of IT assets, business processes, and governance principles used to create a unified and standardized hardware and software environment. ESA is a framework for managing cybersecurity capabilities, policies, and processes to control and mitigate threats. EA and ESA are recognized tenets of organizational transformation and IT

management in both public and private organizations and when implemented effectively can optimize mission performance and Agency strategic outcomes.

In promoting a risk management approach to cybersecurity, NIST describes Enterprise Architecture and Enterprise Security Architecture as being “tightly coupled.” For example, NIST recommends that organizations use security controls as a way to mitigate identified cyber risks.⁷ Specifically, the NIST EA control—known as Program Management 7 (PM-7)—requires that information security be integrated into an organization’s EA to ensure that security considerations are consistent with organizational risk management and cybersecurity strategies. Further, NASA policy, mirroring federal guidance, states that all IT investments made at the enterprise, mission, program, project, and Center levels shall align with the Agency EA.⁸ This policy is intended to address the problem of having a wide variety of IT systems developed in isolation without considering how they might be used with future technologies. Such systems generally lack coordination and planning across the enterprise and therefore could present a security risk.

NIST addresses ESA in CA-1 (Certification, Accreditation, and Security Assessment), which describes the assessment and authorization (A&A) process. A crucial foundation for effective cybersecurity, A&A is a thorough review designed to ensure an IT system meets cybersecurity requirements. At NASA, A&A is required for new systems and annually for all existing systems.

A&A consists of a review of security policies and procedures (management controls); physical facility infrastructure (operational controls); and network testing, server testing, application security testing, penetration testing, and scanning (technical controls). The assessment phase of the process is meant to identify and mitigate security weaknesses; the authorization phase prompts the Agency to account for and accept the risks associated with the IT system under review and to grant that system approval to operate for a specified period of time. A typical A&A package contains at least half a dozen components—such as security and configuration management plans—though significantly more documentation is required if the system contains sensitive data.⁹

Cybersecurity Management at NASA

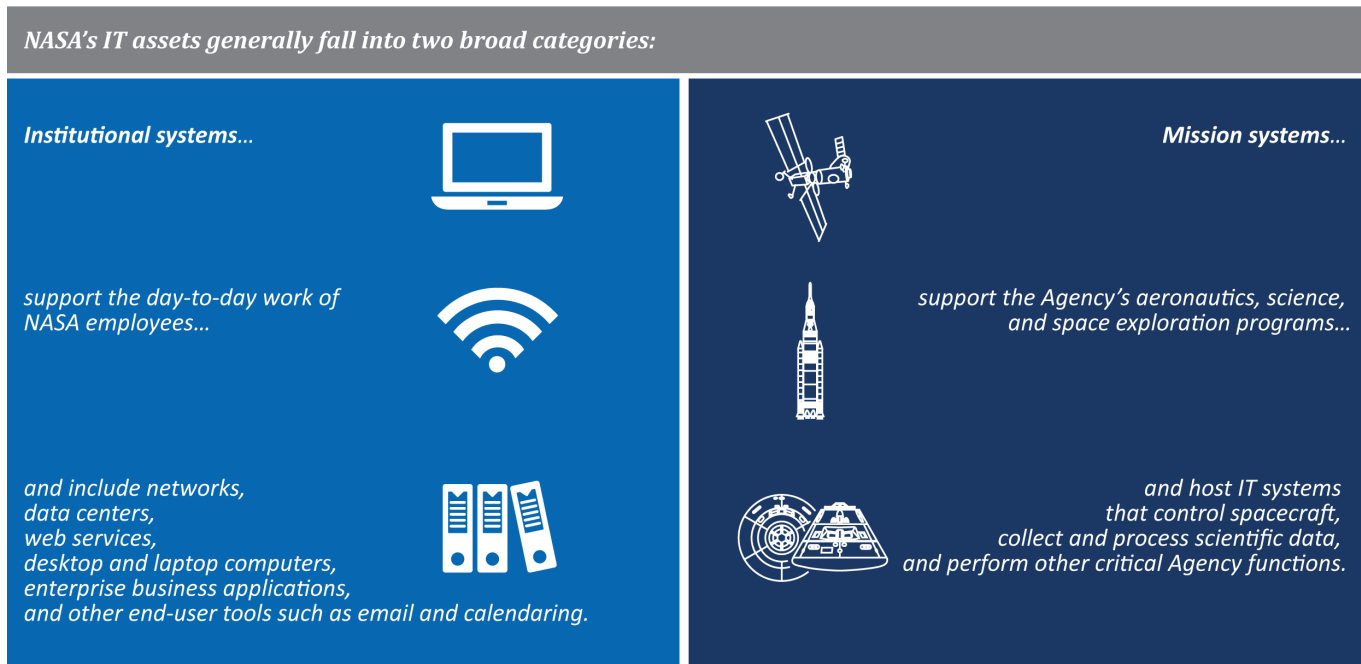
NASA’s IT assets generally fall into two broad categories: institutional IT assets and mission IT assets. Institutional systems support the day-to-day work of NASA employees and include networks, data centers, web services, desktop and laptop computers, enterprise business applications, and other end-user tools such as email and calendaring. Mission systems support the Agency’s aeronautics, science, and space exploration programs and host IT systems that control spacecraft, collect and process scientific data, and perform other critical Agency functions. For example, the Deep Space Network, operated by JPL, is a mission system that supports interplanetary spacecraft missions. Figure 2, shown below, depicts the categories of NASA IT assets.

⁷ NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

⁸ NASA Procedural Requirements (NPR) 2830.1A, *NASA Enterprise Architecture Procedures* (December 19, 2013).

⁹ Examples of sensitive data include export control material, social security numbers, and classified government documents.

Figure 2: Institutional IT Systems vs. Mission IT Systems



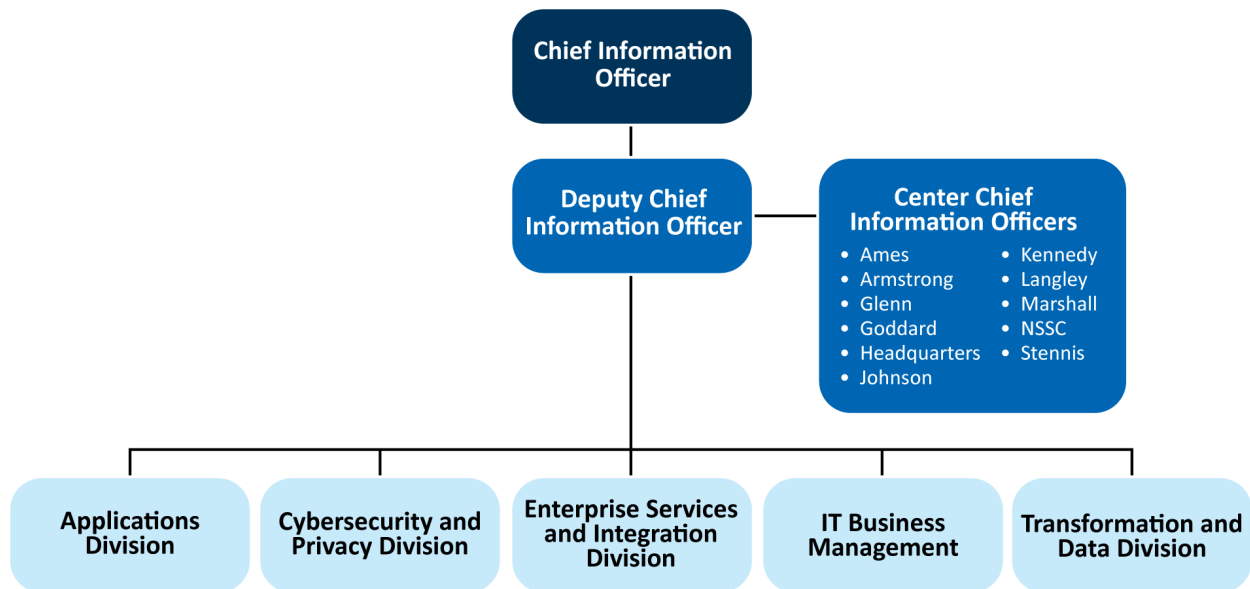
Source: OIG depiction of NASA IT systems categories.

On paper, NASA's cyber risk management is strictly hierarchical, but in reality project and organization dynamics are more complex. For example, the Agency's organizational structure has three primary levels with varying responsibilities—and numerous lines of funding control—for cybersecurity management:

1. *Institutional cyber management.* Located primarily at NASA Headquarters and responsible for providing NASA's strategic direction, the OCIO has overall responsibility for information technology such as email, help desk functions, and security capabilities that support the entire NASA workforce. Within OCIO, the Cybersecurity & Privacy Division (CSPD) operates with a staff of approximately 120, managing activities such as the cybersecurity continuous monitoring infrastructure, cybersecurity and privacy risk, policy development and the Security Operations Center (SOC).¹⁰ CSPD is also responsible for developing, implementing, and maintaining NASA's Enterprise Security Architecture. The OCIO organizational structure is shown in Figure 3.

¹⁰ CSPD utilizes a matrixed workforce structure in which its staffing is augmented by Center personnel. For example, of the 120 cyber-related professionals, approximately 9 percent are direct reports to CSPD. The SOC is responsible for providing an enterprise-wide ability to identify and respond to security incidents through its monitoring of institutional NASA networks and systems.

Figure 3: Office of the Chief Information Officer



Source: NASA

2. *Mission-based cyber management.* NASA has four mission directorates, each led by an Associate Administrator.¹¹ The mission directorates fund their own computer networks and IT personnel; therefore, in most cases, mission directorate personnel rather than OCIO staff have visibility over the operational and security aspects of mission networks. For example, mission directorate personnel determine risk and risk acceptance for networks used for the International Space Station and interplanetary satellite missions such as Juno and the Curiosity Mars rover.¹² Generally, the scope of mission IT includes items with specialized IT (software, hardware, cybersecurity, or other IT services) configured for a specific mission purpose, function, or requirement.
3. *Center-based cyber management.* Each NASA Center Director is responsible for managing operations at their Center and for determining how best to support the programs and projects located there.¹³ This local authority applies to both institutional and mission IT systems. Notably, the NASA OCIO has no direct control over the implementation and enforcement of Center cybersecurity operations—including the network and systems access authorization process. Instead, the Center Chief Information Security Officer (CISO) is responsible for local cybersecurity and serves as the primary interface between the Senior Agency Information

¹¹ NASA's four mission directorates are Aeronautics Research, Human Exploration and Operations, Science, and Space Technology.

¹² The Juno mission, which began orbiting Jupiter in July 2016, improves NASA's understanding of the planet's origins and evolution by mapping its gravity and magnetic fields and observing the composition of its atmosphere. The Mars Science Laboratory, and its rover Curiosity, has been operating on the Red Planet since August 2012.

¹³ NASA consists of a Headquarters office in Washington, D.C.; nine geographically dispersed Centers; JPL; and nine component facilities and testing sites such as the Katherine Johnson Independent Verification and Validation Facility and the White Sands Test Facility.

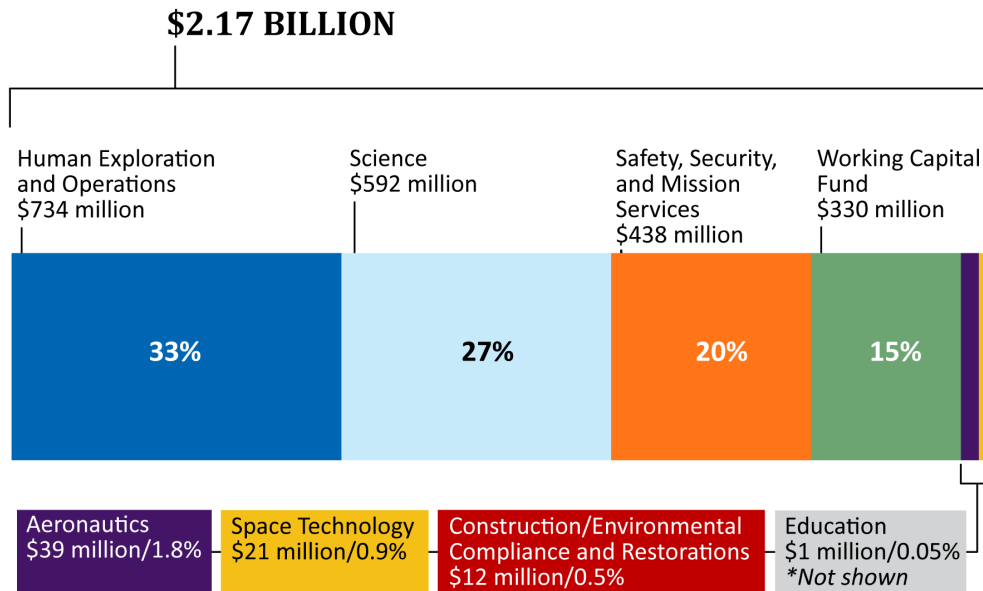
Security Officer (SAISO) located at Headquarters and Center information security functions. Regardless of the Agency's organizational structure, all IT systems are required to follow NASA and NIST guidance and adhere to the A&A process, although how that process is conducted varies across the Agency.

Cybersecurity Spending at NASA

NASA's planned IT spending is about \$2.2 billion a year, or about 10 percent of its overall budget, a figure commensurate with similarly sized federal agencies. However, the proportion NASA spends on IT varies across missions. Figure 4 shows NASA's planned cyber spending for fiscal year (FY) 2021 by organization.

In FY 2020, the OCIO spent \$278 million on IT, \$74 million of which was budgeted for institutional cybersecurity. Separate from the OCIO, mission offices in FY 2020 invested \$169 million on mission-based cyber management at locations around the country.

Figure 4: NASA's IT Portfolio (FY 2021)



Source: NASA

Note: Working Capital is a revolving fund that operates as an accounting entity in which the assets are capitalized and in which all income is derived from the operations of its activities. The fund is available to finance continuing operations without fiscal year limitations.

Major OCIO Initiatives Impacting Cybersecurity

Over the past few years, the OCIO has worked to improve NASA's cybersecurity and IT governance. In September 2019, NASA updated its IT Strategic Plan, which identifies critical activities, milestones, and resources needed to manage IT as a strategic resource. To further improve its IT operating model, the OCIO is currently working through two important initiatives:

1. Mission Support Future Architecture Program (MAP). Traditionally, services such as IT, human resources, finance, and procurement have been managed and operated separately at each NASA Center and at Headquarters. MAP—an ongoing management review—is intended to improve these mission support services by moving the Agency toward an enterprise computing model that would centralize and consolidate IT capabilities, such as software management and cybersecurity. MAP does not, however, address how mission or Center IT systems are managed; it only addresses IT systems that fall into the Agency's institutional category. The OCIO expects to complete its MAP assessment during 2021, with implementation in January 2022.
2. The upcoming Cybersecurity and Privacy Enterprise Solutions and Services (CyPRESS) Contract. One aim of the Agency's planned CyPRESS contract is to eliminate duplicative cyber services and the need for Center-based IT security contracts. Although not formally part of the MAP initiative, CyPRESS is expected to work in concert with MAP as an enterprise-wide security service delivery model. The OCIO anticipates awarding the contract by February 2022.

EFFECTIVENESS OF NASA'S CYBERSECURITY EFFORTS LIMITED BY A DISORGANIZED APPROACH TO ENTERPRISE ARCHITECTURE

NASA's ability to prevent, detect, and mitigate cyber-attacks is limited by a disorganized approach to the Agency's Enterprise Architecture. Enterprise Architecture and Enterprise Security Architecture—the blueprints for how an organization analyzes and operates its IT and cybersecurity—are crucial components for effective IT management. Enterprise Architecture has been in development at NASA for more than a decade yet remains incomplete while the manner in which the Agency manages IT investments and operations remains varied and ad hoc. Overall, a fragmented approach to IT, with numerous, separate lines of authority, has long been a defining feature of the environment in which cybersecurity decisions are made at the Agency. The result is an overall cybersecurity posture that exposes NASA to a higher-than-necessary risk from cyber threats.

NASA's Enterprise Architecture and Enterprise Security Architecture

EA and ESA are a basic tenets of effective IT management. Used together, they can help organizations align enterprise-wide strategic objectives and shared IT infrastructure with a careful approach to cyber risk and overall cybersecurity.

Enterprise architecture (EA) is a blueprint of IT assets, business processes, and governance principles used to create a unified and standardized hardware and software environment. EA describes how an organization's information technology systems operate today, how they are intended to operate in the future, and a road map for the transition. A strong architecture also should document the current and desired relationships among business and management processes and information technology. In computing, the term "enterprise" means a centralized structure, where the IT organization manages the technology—for instance, executing tasks related to software, patching, and security—for the entire organization. EA focuses on understanding the elements that make up the enterprise and how those elements—people, process, business, and technology—relate to each other. In addition, EA is intended to integrate logical elements (integrated functions, applications, systems, users, work locations, and information needs and flows) with technical elements (hardware, software, data, communications, and security). Numerous branches of IT management, such as end user computing, communications, and, importantly, cybersecurity, feed into the overall strategic effort of a well-developed EA. The primary purpose of NASA's EA is to align all the Agency's business, financial, scientific, and engineering needs with technology infrastructure and resources required to support its mission and improve overall IT performance. NASA's Chief Enterprise Architect, residing within the OCIO, is responsible for managing the EA and developing guiding principles, procedures, and technical standards to create an integrated, Agency-wide perspective.

Enterprise Security Architecture (ESA)—a subset of EA—identifies and integrates cybersecurity into the overall EA. The ESA aligns NASA’s enterprise security programs, investments, and capabilities with the Agency’s business needs and strategic goals. NASA’s ESA is based on the NIST framework and has been adjusted to incorporate recommendations from leading IT consulting firms. The Senior Agency Information Security Officer (SAISO) and the Cybersecurity & Privacy Division (CSPD)—both housed within OCIO at Headquarters—have oversight of cybersecurity requirements throughout the Agency’s IT portfolio. Meanwhile, Center CIOs and Center Chief Information Security Officer (CISO) are charged with ensuring all information systems, organizations, and personnel at their respective Centers comply with cybersecurity requirements. ESA does not own a majority of IT services; instead, ESA provides cybersecurity support for services such as software applications, cloud computing, and network capabilities throughout the Agency.

Efficient and effective safeguarding of NASA’s data and assets poses a continuing challenge due to the breadth, fragmentation, and complexity of the Agency’s data and infrastructure. In 2005, we first reported that the NASA OCIO was developing requirements and plans for an enterprise-wide IT architecture and associated management processes. At the time, we cautioned that until those efforts were fully integrated into the budget and operations for each mission directorate and Center, the ability of the CIO to have insight into and influence over IT organizations, their operations, and their budgets would be limited. Similarly, the Government Accountability Office (GAO) recommended in September 2012 that NASA improve measurement and reporting of its EA outcomes and in November 2013 recommended that 100 percent of IT investments—meaning both institutional and mission IT—should be reflected in NASA’s EA.¹⁴ In October 2017, we reported the Agency’s enterprise architecture remained immature after a decade-long improvement effort. And in recent interviews, NASA’s Chief Enterprise Architect explained that neither the 2012 nor 2013 GAO recommendations will be closed any time soon because the Agency wants to give the MAP process more time to progress. In the meantime, EA and ESA will continue to be implemented ad hoc across the Agency.

Despite these shortcomings, over the past several years the OCIO has taken positive steps to improve NASA’s overall cybersecurity program and posture, including implementing the Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) program. First implemented in 2016, these tools help identify and monitor assets connected to the networks and support patch and vulnerability management. CDM deployment is now complete across NASA’s institutional network, with mission network completion scheduled for the fourth quarter of FY 2021. With CDM completion, the Agency will enhance its cybersecurity capabilities by having a more complete picture of assets connected to its networks.

Likewise, the Agency made progress in the areas of identity management and authentication which provide visibility into who and what is connected to the institutional network. NASA requires 100 percent of privileged users to sign in with Personal Identity Verification (PIV) credentials before using its IT assets.¹⁵ For example, privileged users might be able to install or remove software, upgrade the operating system, or modify application configurations. Also, they might have access to files not normally accessible to non-privileged users. Importantly, in 2019 NASA met the 90 percent Federal

¹⁴ *Organizational Transformation: Enterprise Architecture Value Needs to Be Measured and Reported* (GAO-12-791, September 2012); *Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings* (GAO-14-65, November 2013).

¹⁵ Privileged users have more IT system authority than ordinary (non-privileged) users.

Information Security Modernization Act (FISMA) Risk Management Assessment target of unprivileged users being required to utilize PIV.

Lastly, having organization-wide governance and appropriate resources is essential to mitigating cybersecurity risk. In September 2019, NASA updated its IT Strategic Plan, which identifies critical activities, milestones, and resources needed to manage IT as a strategic resource.

Management of EA and ESA is Disjointed

Internal management structures and funding authorities contribute to the disjointed stature of EA and ESA at NASA. For example, we found that although CSPD (housed within OCIO) is responsible for managing NASA's cybersecurity posture and compliance, the Division's authority to enforce a cybersecurity baseline is limited because of organizational boundaries. Adding to this disjointed management, multiple groups—including Center architecture engineering teams and enterprise teams—perform similar EA activities, leading to duplication of effort, infrastructure, and services.

OCIO's internal organizational structure—where EA and ESA are separate entities within the office—is also problematic. EA is located in the Enterprise Services and Integration Division, while ESA is located in the Cybersecurity and Privacy Division. In our opinion, this fragmented organizational structure complicates effective cybersecurity. The current approach, characterized by divided and overlapping lines of responsibility, ignores the reality that cybersecurity requires an integrated approach across all aspects of the Agency's activities and operations. Each Division has its own set of operational goals and management personalities who historically have not shared a similar view on the role of EA, the level of integration between EA and ESA, or the depth and breadth of an enterprise-wide EA approach. This history has resulted in ESA efforts being driven autonomously because the EA roadmap lacks a cohesive alignment across mission and institutional IT boundaries. As stated above, NIST describes EA and ESA as being highly dependent on one another.

According to the OCIO Enterprise Architect and Enterprise Security Architect, integration of cybersecurity into the overall IT infrastructure is nascent across the enterprise. In our judgement, NASA's management approach to EA and ESA should be formally integrated to reduce cybersecurity risk and provide a 360-degree view of its overall effectiveness. A comprehensive EA includes careful consideration of cybersecurity and requires a collaborative effort between the Enterprise Architect and Enterprise Security Architect, as both are responsible for the Agency's overall cybersecurity preparedness.

Further complicating matters is the manner in which IT and cybersecurity are funded on NASA's mission networks. Funding for IT security associated with many NASA programs and projects is embedded in the cost of the underlying mission and may duplicate enterprise-wide activities such as the Security Operation Centers (SOC). For example, in addition to the Agency-funded and -operated SOC that monitors institutional IT operations, four additional entities performing SOC-like activities are operated by missions. IT officials told us having redundant services doesn't make monetary sense and generally provides little additional cyber protection.

The long-standing practice of having missions and Centers with independent budgets and sometimes competing interests impedes the Agency's ability to build a complete EA. Moreover, balancing the competing interests of IT security versus network access remains a challenge. Officials explained that while NASA has adopted the Trusted Internet Connection (TIC) program to assist in protecting its

network, in some cases missions do not use TIC because of resource demands.¹⁶ Cybersecurity, in particular, is hampered because ESA does not have much influence within the Agency's management structure. Unlike the Office of Safety and Mission Assurance, for example, the OCIO does not have technical authority to concur with a mission's lifecycle plan, even though the plan includes details on how the mission has assessed and plans to mitigate cybersecurity risk. We also noted, based on our interviews with Agency personnel, that OCIO's counsel and expertise are often not sought when missions are in the planning stage, resulting in increased cyber risk due to their unfamiliarity with NIST requirements. For example, in recent audits we found numerous instances of system security plans lacking the required measures and information such as system categorization, risk assessments, and system boundary descriptions—essential elements for identifying and managing cyber risk. Importantly, an imprecise system security plan directly impacts the requirements and controls needed to address specific cyber risks within the IT environment.

Agency officials indicated that security is built into EA planning for both institutional and mission systems. However, the degree to which cybersecurity is considered when developing new IT systems and managing existing ones varies widely, resulting in a complex collection of inefficient, potentially incompatible cybersecurity solutions. NASA's SOC provides a prime example of the problems that this type of cybersecurity environment can pose. While the SOC has visibility into NASA's entire institutional network, it has limited knowledge of and visibility into mission networks. In most cases, the responsibility for network and asset protection remains entirely with the missions, with the SOC playing no role in assessing and detecting threats but retains responsibility in the event of a cybersecurity incident. However, without knowledge of specific applications, operating systems, or other device information, the SOC is severely limited in its ability to assist the missions or to correlate event data across institutional and mission network boundaries. Furthermore, because NASA, government, industry, and academia work together at numerous Centers and other locations, information security becomes especially challenging as each component has interdependencies and follows its own set of IT security requirements. It is important to note that the OCIO—housed at NASA Headquarters, responsible for the overall implementation of cybersecurity measures at the Agency, and controller of institutional systems—does not have oversight or control over cybersecurity decisions within the Agency's mission systems.

NASA officials acknowledged that not all missions and partners have IT practices in line with the Agency's ESA. For example, in some cases network and communications drawings lack detail and are not integrated with the enterprise security architecture. Such drawings are important for determining interdependencies—how the parts of a computer network (servers, software, and data) interact to assure the security of the network and its communications.

¹⁶ The goal of Trusted Internet Connections is to document existing public internet connections on government networks and create plans to limit their number so data coming in and out can be monitored and analyzed more effectively. Over time, greater bandwidth demands, transport encryption, and perimeter services were placed on agency TIC access points beyond their ability to scale. The growing demands on the enterprise perimeter and degraded performance increased the cost and decreased the effectiveness of the TIC initiative when using cloud services. As a result, NASA worked with the Department of Homeland Security to develop a solution to bring data from satellites straight to the cloud for sharing with researchers.

EA and ESA Priorities Exclude Important Systems

One cause of the disorganization around EA and ESA is NASA's practice of prioritizing institutional systems and high-risk missions such as the Space Launch System and the International Space Station, leaving cybersecurity for other mission systems as a secondary concern, with those systems integrated into the EA and ESA as time and resources permit.

While the OCIO has responsibility for institutional governed IT, missions are left to their own discretion to interpret and implement requirements and, importantly, absorb costs associated with cybersecurity. For example, larger programs such as Orion and the Joint Polar Satellite System are better at managing cybersecurity while smaller missions such as CubeSats, tend to struggle because of their specialized technology and lack of assets (people, tools, and funding) to devote to cyber efforts.¹⁷ Specifically, the larger programs understand NIST guidance for security categorization, and the selection and implementation of security controls; generally, smaller programs lack familiarity and expertise with these complex cyber concepts.¹⁸ Agency officials explained that the smaller missions tend to put cybersecurity last on their "to-do" lists, with science—not IT—remaining their first priority. In cybersecurity, though, the fortress is only as strong as its weakest entry point. We discuss specific security controls in detail in Appendix B.

Ultimately, effective cybersecurity depends on the extent to which security controls are well designed, implemented correctly, operate as intended, and produce the desired outcomes with respect to meeting cybersecurity requirements for the organization's data and information systems. NASA officials told us that if cybersecurity is not recognized early in the planning cycle and noted in the policy and process documents, it tends to be overlooked. In our judgement, without stronger requirements to include cyber concerns throughout all of the Agency's operations, NASA will continue to be exposed to an elevated risk of cyber-attack.

¹⁷ Orion is the capsule that will carry NASA astronauts to the moon and other deep-space destinations; the Joint Polar Satellite System is a polar-orbiting operational environmental satellite system; a CubeSat is a type of space research nanosatellite with a base dimension of 10x10x11 centimeters (one "Cube" or "1U"), or approximately four inches.

¹⁸ A security control is a protective measure or safeguard against threats.

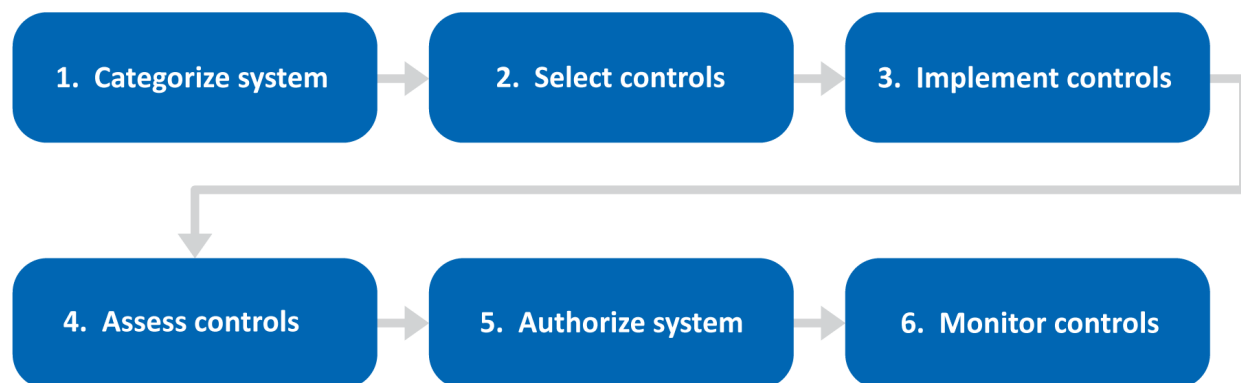
NASA'S ASSESSMENT AND AUTHORIZATION PROCESS REMAINS INCONSISTENT AND INEFFECTIVE

NASA conducts its assessment and authorization (A&A) of IT systems inconsistently and ineffectively, with the quality and cost of the assessments varying widely across the Agency. These inconsistencies can be tied directly to NASA's decentralized approach to cybersecurity, which has persisted for more than a decade. NASA is currently planning to enter into a new Cybersecurity and Privacy Enterprise Solutions and Services (CyPRESS) contract intended to eliminate duplicative cyber services, which could provide the Agency a vehicle to reset the A&A process to more effectively secure IT systems.

The Assessment and Authorization Process

Organizations conduct A&A on their IT systems to ensure the systems meet cybersecurity requirements. At NASA, A&A is required for newly introduced systems and also annually for all other systems. A&A is generally conducted by both NASA civil servants, who provide oversight of compliance, documentation, and reporting, and contractors, who to perform the independent technical assessments. The end products of A&A include authorization to operate, risk-based decisions on the application of individual controls, and a plan of action and milestones to address identified deficiencies. Modeled after the NIST Risk Management Framework, the A&A process is comprised of six key tasks, as shown in Figure 5. It is important to note that the main resource required to conduct A&A is labor—the process is largely a function of staff hours and requires a variety of cybersecurity knowledge and skillsets.

Figure 5: Annual Assessment and Authorization Process



Source: OIG depiction of Assessment and Authorization Process.

Guidelines and Requirements for A&A

NIST has an extensive library of documents to assist government and private sector organizations in managing their information technology assets. Included in this library are several publications specifically detailing actions to be taken when assessing systems for risk and authorizing them to operate. These publications provide a catalog of security and privacy controls needed to strengthen and support critical infrastructure from a diverse set of threats and risks, including hostile attacks, human error, natural disasters, structural failures, foreign intelligence entities, and privacy risks. This foundational control guidance details specific risk management activities to be carried out in support of a comprehensive collection of security controls including those supporting EA, ESA, and A&A. However, while this guidance is either required or suggested for use by NASA, OIG audits have consistently identified instances where the NIST guidance was not followed during system security plan development. Moreover, private sector subject matter experts suggest that operating similar lines of business separately is ineffective and wasteful, leading to inconsistent and untimely decision making and compliance issues across the organization, a lack of transparency regarding vendor performance, missed opportunities to apply leverage when negotiating new work, poor operational discipline, and failure to coordinate and make use of expertise that exists within the organization.¹⁹

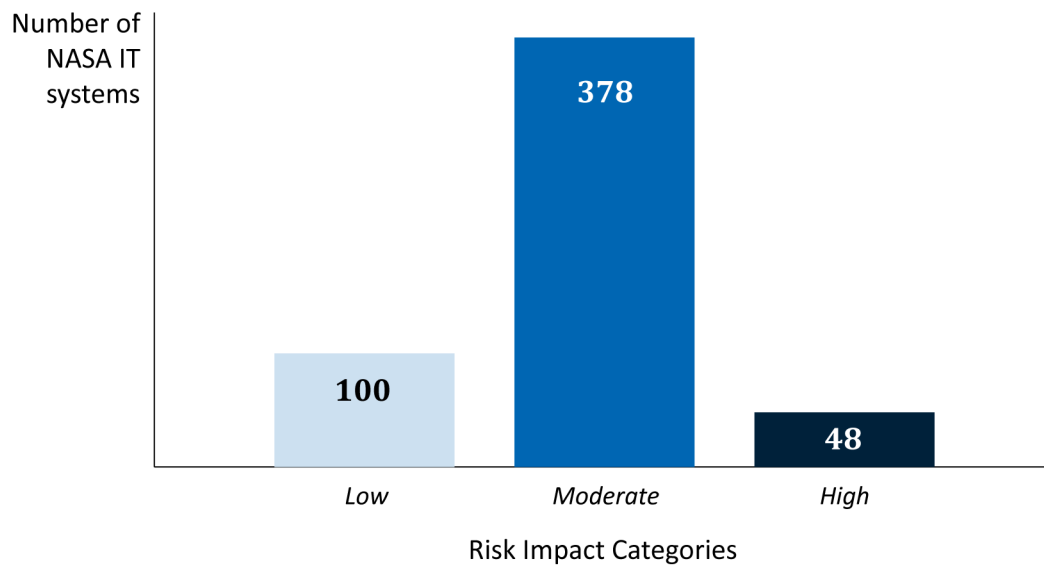
- NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- Federal Information Processing Standards (FIPS) 199, *Categorizing Federal Information Systems*
- NIST SP 800-60, Volumes I and II, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-53 and 800-53(a), *Security and Privacy Controls for Information Systems and Organizations; Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*

Overall Inconsistencies in NASA's A&A process

NASA's IT inventory in 2020 included 526 systems classified in one of three risk exposure levels as shown in Figure 6.

¹⁹ Founded in 1926 by University of Chicago professor James O. McKinsey, McKinsey & Company is a management consulting firm that advises on strategic management to corporations, governments, and other organizations. The whitepaper, *Seven levers for corporate- and business-function success: Consolidation (lever 2)* (July 2014), delves into successes organizations can achieve through consolidation of like processes and functional lines of business.

Figure 6: NASA Systems Inventory



Source: OIG representation of NASA data.

We found that NASA’s A&A process is not conducted consistently across the Agency. Centers have varying cost models and charge system owners—the missions that house the IT systems and thus incur the requirement to conduct A&A—different rates for the assessments. For example, system owners at JPL and Langley Research Center are provided the A&A service free-of-charge as part of existing Center-based contracts. At Goddard Space Flight Center, institutional system owners are provided the A&A service at no cost while mission system owners are charged varying rates for the assessment based on the categorization of the system and other factors. Meanwhile, at Kennedy Space Center (Kennedy), organizations that own non-Kennedy mission or enterprise institutional systems are charged for A&A, while owners of Center-based systems are not. The exception is the Exploration Ground Systems, a Kennedy managed program that supplements the A&A cost based on their large volume of security plans.²⁰

Assessment Process Historically Conducted Poorly

We also noted that the assessment process misses key aspects of data protection, lacks staff with an understanding of the complexities of mission systems or criticality analysis, and is viewed by some individual organizations as unduly burdensome. Taken together, these factors have led to frustration and added work, and have resulted in some NASA organizations questioning the value of the A&A process. In our opinion, all of this leads to an environment where inappropriate levels of risk are accepted simply to avoid the perceived burdens associated with the A&A process.

Over the past 6 years we have reported that certain types of data have been ignored or discarded as irrelevant during the A&A process, leaving systems incorrectly categorized at lower risk impact levels than their criticality requires. For instance, in a March 2015 report we found a system used for command and control of spacecraft incorrectly categorized as if it did not provide command and

²⁰ The Exploration Ground Systems Program is responsible for major infrastructure components supporting ground processing and launch preparations for the integrated Orion/Space Launch System (SLS) capsule and launch vehicle.

telemetry for the spacecraft; this system later fell victim to a cyber incident.²¹ In another instance, an audit found large numbers of disparate systems of differing risk impact levels being grouped into a single security plan, resulting in inappropriate application of security controls.²² Similarly, we have previously reported categorization decisions for IT systems that appeared arbitrary in nature and not based on the established criteria.²³ In particular, one such finding noted that NIST guidance was not taken into consideration when assigning risk impact levels. Further, our February 2021 FISMA report noted that control assessments were not consistently comprehensive.²⁴ Moreover, as of March 2021 we identified 35 systems whose authority to operate has expired and 82 systems that are overdue for contingency plan testing.²⁵ According to Agency policy, NASA systems are to be categorized in accordance with NIST guidance, and any errors in categorization should be identified and corrected during the A&A process. Properly categorizing systems is critical for ensuring NASA systems and data maintain appropriate levels of confidentiality, integrity, and availability and is a fundamental step that should be reviewed closely during A&A. Additionally, our past reports have identified security control deficiencies such as (1) data protection controls that can be directly tied to weaknesses in categorization step of the A&A process, (2) boundary controls and interconnections which can be directly attributed to a lack of criticality analysis or comprehensive assessment practices, and (3) lack of visibility across the enterprise which can be attributed to a lack of consistency and dedicated resources. With a focused and comprehensive assessment, it is likely that these deficiencies would be identified and corrected during the A&A process.

Disjointed Management Structure for A&A

Adding to the overall inconsistency in the A&A process is the disjointed management structure for conducting these assessments across the Agency. A&A is a critical function that requires dedicated staff with diverse cybersecurity knowledge and skillsets, but the civil service personnel tasked with overseeing A&A at the Centers have other cybersecurity responsibilities. The current practice at NASA is for each Center to hire external, independent A&A assessors through Center-based contracts, which contradicts management best practices that suggest consolidating like functional lines of business within an organization. Operating in this manner adds to existing frustration with the A&A process and exacerbates existing IT governance challenges. Responsible officials explained that the A&A process is often viewed as cumbersome and arbitrary, and that the assessor's technical inputs into the process are, as a byproduct of that viewpoint, sometimes without value. As we have noted in prior reports, the NASA SAISO, who is responsible for the Agency's cybersecurity program, does not have insight into the cost, skillsets, and staffing for A&A across Centers even though the individual is required to provide oversight and report to OMB on NASA's cybersecurity posture.

²¹ NASA OIG, *NASA's Management of the Deep Space Network*, ([IG-15-013](#), March 26, 2015).

²² NASA OIG, *Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure* ([IG-17-011](#), February 8, 2017).

²³ NASA OIG, *NASA Management of Distributed Active Archive Centers*, (IG-20-011, March 3, 2020); *NASA Management of the Near Earth Network*, ([IG-16-014](#), March 17, 2016); and IG-15-013.

²⁴ NASA OIG, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Communications System* ([IG-21-013](#), February 16, 2021).

²⁵ Data obtained through NASA's Risk Information, Security, and Compliance System (RISCS) maintained by the OCIO. RISCS is a data repository that contains an inventory of the Agency's hardware and software, including system security and contingency plans for each information system.

The inconsistencies in cost, process, and performance related to the A&A process tie directly to NASA's historically decentralized approach to cybersecurity. While the Agency is gradually moving toward an enterprise approach, Centers continue to manage their A&A processes using differing models under separate contracts with varying costs passed down to NASA organizations. A dedicated, enterprise-level A&A process managed as a single functional line of business would promote consistency in cost and practices, strategized allocation of needed skillsets, alignment with CSPD's vision for enterprise protection, and criticality analysis across NASA's diverse systems inventory. Best practice and evidence collected over nearly a decade of reviewing NASA's cybersecurity posture dictate needed changes in the way NASA approaches assessment and authorization. The A&A function—a NIST Risk Management Framework requirement—is designed to be applied in a consistent manner across all NASA systems, with emphasis on robust criticality analysis including context diagrams of low-, moderate-, and high-impact systems and their environments.

A&A Consolidation Has Potential for Cost Savings

The decentralized nature of NASA's operations coupled with the Agency's long-standing culture of autonomy hinders CSPD's ability to gather pertinent data regarding A&A costs, staffing, and cybersecurity skillsets available Agency-wide. CSPD is attempting to collect and analyze this information, without success at the time of this report. In an effort to determine the overall annual costs for A&A, we analyzed costs at two NASA Centers. In FY 2020, Goddard conducted A&A on 38 IT systems using a part-time staff of 4 contractors and 4 civil servants at a cost of \$765,000. That same year, Kennedy conducted A&A on 38 systems with a staff of 3 contractors and 2 civil servants at cost of \$554,000. Extrapolating these costs to the universe of NASA's 526 IT systems, we estimated overall annual costs for A&A are approximately \$6 to \$7 million. In our opinion, the Agency should be able to achieve cost savings by consolidating the A&A process into a dedicated enterprise function rather than its current decentralized form that operates under numerous, disparate contracts. In addition, by dedicating a staff of experts to the process NASA could dramatically improve the quality of its A&A outcomes, thereby improving the Agency's overall cybersecurity posture.

Moving forward, NASA has a unique opportunity as the Agency is currently in the planning process for the new Cybersecurity and Privacy Enterprise Solutions and Services (CyPrESS) contract (expected to be awarded in February 2022) that will include enterprise IT support services. Ensuring integration of A&A into the CyPrESS contract will provide much-needed consistency and dedicated resources and will help NASA position itself to detect cyber deficiencies and mitigate them early in each IT system's lifecycle.

CONCLUSION

Attacks on NASA networks are not a new phenomenon, although attempts to steal critical information are increasing in both complexity and severity. As attackers become more aggressive, organized, and sophisticated, managing and mitigating cybersecurity risk is critical to protecting NASA's vast network of information technology systems from malicious attacks or breaches that can seriously inhibit the Agency's ability to carry out its mission. Although NASA has taken positive steps to address cybersecurity in the areas of network monitoring, identity management, and updating its IT Strategic Plan, it continues to face challenges in strengthening the foundational cybersecurity efforts related to EA and modernizing the A&A process. Specifically, the Agency's cybersecurity preparedness is strained due to ambiguity surrounding the requisite technical integration between EA/ESA, gaps in mission visibility, and inconsistent and ineffective practices around the A&A process. When system owners view A&A as a burden rather than a benefit, poor risk management decisions are inevitable.

Adopting an integrated EA/ESA and developing an effective enterprise-level A&A process would not only dramatically improve situational awareness, but would also enable NASA's decision makers to effect positive change on the Agency's cybersecurity posture. Officials would be better positioned to gauge risk, anticipate disruptions, and determine where investment in additional resources or other changes are needed. We are hopeful that the MAP initiative and CyPRESS contract will provide much needed progress on these issues. However, history has shown that driving change at NASA can be an uphill effort when management decisions hinge on the Agency's federated model, with multiple lines of independent authority among headquarters and geographically dispersed missions and Centers. This is especially true when issues like IT management and cybersecurity cross organizational boundaries and where competing interests and independent budgets come into play. In our opinion, NASA must act decisively to deploy and adjust its IT security strategies to keep up with evolving cyber threats.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

In order to strengthen NASA's cybersecurity readiness and provide process continuity and improved security posture for NASA's systems, we recommended the Associate Administrator and the Chief Information Officer:

1. Integrate EA and ESA, and develop metrics to track the overall progress and effectiveness of EA.
2. Collaborate with the Chief Engineer on strategies to identify and strengthen EA gaps across mission and institutional IT boundaries.
3. Evaluate the optimal organizational placement of the Enterprise Architect and Enterprise Security Architect during and after MAP implementation to improve cybersecurity readiness.
4. Determine each Center's annual cost for performing independent assessments, including staffing, during the A&A process for NASA's 526 systems.
5. Develop baseline requirements in the planned CyPrESS contract for a dedicated enterprise team to manage and perform the assessment process for all NASA systems subject to A&A.

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

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

Major contributors to this report include Tekla Colon, Program Director; Scott Riggenbach, Project Manager; Linda Hargrove; Christopher Reeves; and Editor Matt Ward.

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 2020 through May 2021 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.

The scope of this audit was NASA's overall cybersecurity posture and related management policies and practices. Our audit objective was to determine if NASA is adequately prepared to identify cybersecurity threats and defend against a major cybersecurity breach. Specifically, we examined:

1. Is NASA's enterprise architecture designed to appropriately assess current and future cybersecurity risks and threats?
2. Is NASA's cybersecurity protection strategy risk-based?
3. Is NASA's cybersecurity resource allocation adequate and appropriately prioritized?
4. How effective is NASA at assessing its risks and implementing basic controls focused on sound cybersecurity practices?

Methodology

To determine whether NASA is adequately prepared to identify cybersecurity threats and defend against a major cybersecurity breach, and to discuss the current status of EA activities and the integration of EA and the ESA functions, we reviewed applicable laws and regulations and interviewed various NASA personnel including the Chief Information Officer (CIO), Associate CIO for Enterprise Services and Integration, Chief Enterprise Architect, OCIO Enterprise Security Architecture lead, and Senior Agency Information Security Officer. In addition to conducting these interviews, we obtained and reviewed Agency EA and ESA documentation including an EA draft NASA Policy Directive.

To gain insight into NASA's cybersecurity strategy, we met with OCIO representatives. We analyzed documentation describing and supporting the cyber processes to identify potential shortcomings and areas for improvement. In addition, we met with the MAP integrator to discuss overall impacts of MAP on the OCIO and effects that it will have on cybersecurity strategy, including the anticipated CyPRESS contract.

To evaluate cybersecurity resource allocation and prioritization, we met with OCIO financial and staffing representatives to discuss budgeting, spending, and staffing activities and concerns. In addition, we obtained and analyzed budgeting and staffing data.

To assess sound cybersecurity practices, we reviewed past cyber breaches, analyzed incident data, and summarized OMB's recently issued FISMA report to Congress describing cyber incidents by attack vector. We interviewed officials to obtain information on actions they have planned or taken to improve NASA's cybersecurity preparedness.

Finally, we relied on the NIST Cybersecurity Framework and 800 Series Special Publications, the Center for Internet Security (CIS) Top 20 Controls, and the Federal Enterprise Architecture for guidance.

We selected 10 CIS Critical Controls that are of particular importance to NASA's cybersecurity. For our analysis, we met with numerous Agency and Center personnel, and collected and analyzed data, policies, procedures, and other documentation including the status of previous IG and GAO report recommendations. For each of the 10 Security Controls reviewed, we compared the control to foundational practices and evaluation criteria and assigned a rating based on NIST Cybersecurity Framework's implementation tiers. See Appendix B for further discussion on security control ratings.

Assessment of Data Reliability

We used limited computer-processed data extracted from NASA's IT and financial systems during the course of this audit. Although we did not independently verify the reliability of this information, we compared it with other available supporting documents to determine data consistency and reasonableness. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations to determine NASA's cybersecurity preparedness. Control weaknesses are identified and discussed in this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have issued 34 reports and testimony of significant relevance to the subject of this report. Reports can be accessed at <https://oig.nasa.gov/> and <https://www.gao.gov/>.

NASA Office of Inspector General

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Communications System ([IG-21-013](#), February 16, 2021).

Congressional Testimony of Paul Martin, NASA Inspector General. *Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19* ([IG CT-2020-1](#), September 18, 2020)

Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices ([IG-20-021](#), August 27, 2020)

Evaluation of NASA's Information Security Program Under the Federal Information Security Modernization Act for Fiscal Year 2019 ([IG-20-017](#), June 25, 2020)

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

NASA's Management of Distributed Active Archive Centers ([IG-20-011](#), March 03, 2020)

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

Audit of NASA's Information Technology Supply Chain Risk Management Efforts
([IG-18-019](#), May 24, 2018)

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

Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation
([IG-18-003](#), November 6, 2017)

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

Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure
([IG-17-011](#), February 8, 2017)

Security of NASA's Cloud Computing Services ([IG-17-010](#), February 7, 2017)

Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation
([IG-17-002](#), November 7, 2016)

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

Final Memorandum, Review of NASA's Information Security Program ([IG-16-016](#), April 14, 2016)

NASA's Management of the Near-Earth Network ([IG-16-014](#), March 17, 2016)

Government Accountability Office

Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed ([GAO-20-126](#), December 12, 2019)

Information Technology: Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity ([GAO-20-311T](#), December 11, 2019)

Information Security: VA and Other Federal Agencies Need to Address Significant Challenges
([GAO-20-256T](#), November 14, 2019)

Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities
([GAO-20-129](#), October 30, 2019)

Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid ([GAO-19-332](#), August 26, 2019)

Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices
([GAO-19-545](#), July 26, 2019)

Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
([GAO-19-384](#), July 25, 2019)

Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes
([GAO-19-288](#), May 17, 2019)

Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation
([GAO-19-131](#)) April 29, 2019

Information Technology: Agencies Need Better Information on the Use of Noncompetitive and Bridge Contracts ([GAO-19-63](#), December 11, 2018)

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

Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption ([GAO-18-211](#), February 15, 2018)

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices ([GAO-17-549](#), September 28, 2017)

Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges
([GAO-17-533T](#), April 4, 2017)

Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems
([GAO-17-518T](#), March 28, 2017)

Cybersecurity: Actions Needed to Strengthen U.S. Capabilities ([GAO-17-440T](#), February 14, 2017)


Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely ([GAO-17-163](#), February 1, 2017)

APPENDIX B: SECURITY CONTROL RATINGS

NIST has defined four Cybersecurity Framework Implementation Tiers that classify organizations according to how well risk management practices have been implemented. Tier 1 organizations have ineffective risk management methods, Tier 2 have informal risk management methods, Tier 3 have structured risk management methods, and Tier 4 have adaptive risk management methods.

To evaluate this subset of Center for Internet Security (CIS) Top Twenty Critical Controls, we interviewed key OCIO staff and requested and reviewed policy, procedural, and other supporting documentation as well as past OIG/GAO reports and recommendations. We assigned a rating to each control based on the NIST Cybersecurity Framework, as shown in the Figure 7.

Figure 7: NASA Security Control Ratings



SECURITY CONTROL	RATING	TIER
Inventory and Control of Hardware Assets	Risk Informed	2
Inventory and Control of Software Assets	Risk Informed	2
Continuous Vulnerability Management	Repeatable	3
Controlled Use of Administrator Privileges	Risk Informed	2
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Repeatable	3
Maintenance, Monitoring, and Analysis of Audit Logs	Repeatable	3
Malware Defenses	Repeatable	3
Boundary Defense	Risk informed	2
Data Protection	Partial	1
Incident Response and Management	Risk Informed	2

Source: OIG Analysis of NASA data

The four NIST Tiers are:

Tier 1: Partial Rating: Cybersecurity risk management is typically performed in an ad hoc/reactive manner. Furthermore, cybersecurity activities are performed with little to no prioritization based on the degree of risk that those activities address. The lack of processes associated with cyber risk management makes the communication and management of that risk difficult for these organizations. As a result, the organization works with cybersecurity risk management on a case-by-case basis because of the lack of consistent information.

Tier 2: Risk Informed Rating: Risk management practices, while approved by management, are typically not established as organizational-wide policies. The awareness of cybersecurity risk exists at the organizational level, but it is not standardized organization-wide, and the information around cybersecurity is only shared informally. A cyber risk assessment may occur, but it is not standard and periodically repeated.

Tier 3: Repeatable Rating: There is an organization-wide approach to managing cybersecurity risk expressed by policy and process. Risk-informed policies, processes, and procedures are defined, implemented, reviewed, and updated regularly based on changes in business requirements and changing threat landscape. There are methods in place to consistently respond effectively to changes in risk, and personnel possess the knowledge and skills to perform their roles. Senior cybersecurity and business-side executives communicate regularly regarding cybersecurity risk.

Tier 4: Adaptive Rating: Cybersecurity practices are adaptive — based on previous and current cybersecurity activities, including lessons learned and predictive factors. They implement a process of continuous improvement—including incorporating advanced cybersecurity technologies and practices, actively adapting to a changing threat and technology landscape. Building on Tier 3, Tier 4 organizations clearly understand the link between organizational objectives and cybersecurity risk. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. These organizations base budgeting decisions on an understanding of the current and potential risk environment. Cybersecurity risk is integrated into the organizational culture and evolves from an awareness of previous activities and continuous awareness.

APPENDIX C: COMMON ATTACK VECTORS

The attack vectors listed in Table 2 are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, with an explanation and example. Notably, it is not uncommon for cyber-attacks to deploy a combination of attack vectors.

Table 2: Common Attack Vector Methods

Vector	Explanation	Example
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	A brute force attack against an authentication mechanism, such as passwords or digital signatures.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation	An attack involving replacement of something benign with something malicious.	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user.	A user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss/Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A lost laptop, smartphone, or authentication token.
Web	An attack executed from a website or web-based application.	A cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

Source: OIG representation of NIST information.

APPENDIX D: MANAGEMENT'S COMMENTS

National Aeronautics and
Space Administration

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



May 13, 2021

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Agency Response to OIG Draft Memorandum, "NASA's Cybersecurity Readiness" (A-20-009-00)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft memorandum entitled, "NASA's Cybersecurity Readiness" (A-20-009-00), dated April 19, 2021.

In the draft memorandum, the OIG makes five recommendations addressed to the Associate Administrator and the Chief Information Officer in order to strengthen NASA's cybersecurity readiness and provide process continuity and improved security posture.

Specifically, the OIG recommends the following:

Recommendation 1: Integrate EA and ESA, and develop metrics to track the overall progress and effectiveness of EA.

Management's Response: Concur. NASA's Office of the Chief Information Officer (OCIO) Mission Support Future Architecture Program (MAP) is establishing in integrated Enterprise Architecture (EA) program that will include enterprise security architecture and explicit performance metrics to track the progress and effectiveness of EA.

Estimated Completion Date: May 31, 2022.

Recommendation 2: Collaborate with the Chief Engineer on strategies to identify and strengthen EA gaps across mission and institutional IT boundaries.

Management's Response: Concur. The NASA Chief Engineer will be a key stakeholder in the MAP EA operating model, which will include collaboration on strategies to identify and strengthen EA gaps across mission and institutional Information Technology (IT) boundaries.

Estimated Completion Date: January 30, 2022.

Recommendation 3: Evaluate the optimal organizational placement of the Enterprise Architect and Enterprise Security Architect during and after MAP implementation to improve cybersecurity readiness.

Management's Response: Concur. The evaluation of optimal organizational placement for EA has been completed and approved by NASA's Mission Support Council. This new EA office, which includes the Enterprise Architect and Enterprise Security Architect, has been elevated within the OCIO organization and now reports directly to the Deputy CIO for Strategy.

As part of MAP implementation, performance metrics will be developed and leveraged to evaluate the effectiveness and success of the overall EA program, including improvements to cybersecurity readiness, both during and after MAP implementation.

Estimated Completion Date: July 29, 2022.

Recommendation 4: Determine each Center's annual cost for performing independent assessments, including staffing, during the A&A process for NASA's 526 systems.

Management's Response: Concur. NASA OCIO will determine the Centers' annual cost for performing independent assessments for NASA's 526 systems.

Estimated Completion Date: December 30, 2022.

Recommendation 5: Develop baseline requirements in the planned CyPrESS contract for a dedicated enterprise team to manage and perform the assessment process for all NASA systems subject to A&A.

Management's Response: Concur. NASA OCIO developed baseline requirements in the planned Cybersecurity and Privacy Enterprise Solutions and Services (CyPrESS) contract for a dedicated enterprise team to manage and perform the security assessments for all NASA systems subject to assessment and authorization (A&A).

Estimated Completion Date: December 30, 2022.

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


3

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

Jeff Seaton

Chief Information Officer

 Digitally signed by JEFFREY SEATON
Date: 2021.05.13 12:10:26 -04'00'

APPENDIX E: REPORT DISTRIBUTION

National Aeronautics and Space Administration

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

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 Space and Science

Senate Committee on Homeland Security and Governmental Affairs

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

House Committee on Oversight and 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-20-009-00)