United States Government Accountability Office

Report to Congressional Requesters

May 2024

NASA CYBERSECURITY

Plan Needed to Update Spacecraft Acquisition Policies and Standards

GAO-24-106624

GAO Highlights

Highlights of GAO-24-106624, a report to congressional requesters

Why GAO Did This Study

NASA's space development project portfolio includes 34 major projects, in which NASA plans to invest more than $83 billion. Spacecraft are operating in a heightened cyber threat environment with increased risks of attack and mission disruption. NASA has identified civil space events that demonstrate the need to better protect spacecraft against cyber threats.

GAO was asked to examine the cybersecurity requirements in NASA contracts for its spacecraft projects. This report assesses the extent to which NASA (1) incorporated cybersecurity in selected spacecraft contracts and (2) determined whether additional cybersecurity updates, if any, are needed to its acquisition policies and standards for spacecraft.

GAO reviewed NASA policies and standards regarding spacecraft cybersecurity. GAO selected a nongeneralizable sample of three spacecraft projects, chosen because they represent different NASA centers and development stages, and include at least one robotic and one human spaceflight project. For these three, GAO analyzed contracts and project documents. GAO also interviewed project and cybersecurity officials.

What GAO Recommends

GAO recommends NASA develop a plan with time frames to update its spacecraft acquisition policies to include essential controls. NASA agreed to update its policies but did not agree to set a plan with dates to do so. Without a plan, GAO maintains it is unknown when implementation would occur. Accordingly, the recommendation remains valid.

View GAO-24-106624. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov, or Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

May 2024

NASA CYBERSECURITY

Plan Needed to Update Spacecraft Acquisition Policies and Standards

What GAO Found

Spacecraft developed by the National Aeronautics and Space Administration (NASA) depend on software and IT, which, in turn, rely on cybersecurity to prevent, detect, and respond to potential cyber incidents. A cyber incident could result in loss of mission data, decreased lifespan or capability of space systems, or the loss of control of space vehicles. Cyber threats and technology change rapidly. In response, the federal government issues government-wide cybersecurity guidelines, such as the National Institute of Standards and Technology's Risk Management Framework.

Source: KanawatTH/stock.adobe.com. | GAO-24-106624

Contracts for the selected NASA projects GAO reviewed required contractors to address cybersecurity, consistent with NASA standards. In 2019, NASA identified a set of cybersecurity requirements for spacecraft to address. For example, NASA requires spacecraft to protect positioning, navigation, and timing systems. The three spacecraft projects GAO reviewed—Gateway Power and Propulsion Element; Orion Multi-Purpose Crew Vehicle; and Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer—started development before 2019. Nevertheless, GAO found these contracts include requirements related to NASA's spacecraft cybersecurity standards. Contracts also required contractors to demonstrate requirements are met through testing.

Since the issuance of its 2019 cybersecurity requirements, NASA has considered, but not yet implemented, updates to its spacecraft acquisition policies and standards. In 2023, NASA issued a space best practices guide containing information on cybersecurity principles and controls, threat actor capabilities, and potential mitigation strategies, among other things. However, this guidance is optional for spacecraft programs. NASA officials explained that one key reason they have not yet incorporated this guidance into required acquisition policies and standards is because of the length of time it takes to do so. GAO acknowledges that the standards-setting process can take time, but it is essential that NASA do so for practices that should be required. However, officials stated that they did not have an implementation plan and time frame to incorporate additional security controls into acquisition policies and standards. As a result, NASA risks inconsistent implementation of cybersecurity controls and lacks assurance that spacecraft have a layered and comprehensive defense against attacks.

Contents

Tables

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CPMO	Chief Program Management Officer
DOD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
HALO	Habitation and Logistics Outpost
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
PNT	positioning, navigation, and timing
PPE	Gateway Power and Propulsion Element
RMF	risk management framework
SPHEREx	Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer

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

May 1, 2024

Congressional Requesters

The National Aeronautics and Space Administration (NASA) depends on IT systems to develop, test, and operate its portfolio of 34 major space development projects. It plans to invest more than $83 billion in these projects, as of 2023. The portfolio includes satellites equipped with advanced sensors to study the Earth, telescopes intended to explore the universe, and spacecraft to transport humans and cargo beyond low Earth orbit. These projects represent significant investments in innovative technology and are attractive targets for malicious actors. Each project involves a range of sensitive data, from intellectual property to the data transmitted by the spacecraft. The security of the systems supporting these projects is vital because of the risks if such data are stolen or manipulated.

In a February 2019 memo, NASA identified threats and vulnerabilities with civil space missions that demonstrated the need to better protect command links for spacecraft.[1] For example, in some instances, spacecraft lost GPS signals necessary to operate the spacecraft. The NASA Associate Administrator directed the NASA Chief Engineer to develop additional protection and incorporate the requirements into agency policy expeditiously. In turn, the Chief Engineer issued a spacecraft protection standard in October 2019.[2]

Incorporating cybersecurity requirements from the earliest stages of an acquisition is typically easier, less costly, and more effective than trying to add cybersecurity protections late in the development. Moreover, because contractors have a key role in designing and building NASA spacecraft and other systems, NASA must communicate its cybersecurity requirements—minimum performance needed to protect its systems against identified threats and vulnerabilities—to its contractors as it would other types of contract performance requirements.

[1] A command link is a connection from transmission at the ground system terminal or space transmitter to receipt by the spacecraft receiver.

[2] National Aeronautics and Space Administration, NASA Technical Standard, *Space System Protection Standard*, NASA-STD-1006, (Jul. 15, 2022) (Revision A).

You asked us to examine the cybersecurity requirements in NASA contracts for its spacecraft projects. Our report addresses the extent to which NASA (1) incorporated cybersecurity in selected spacecraft contracts and (2) determined whether additional cybersecurity updates, if any, are needed to its acquisition policies and standards for spacecraft. The review focused on spacecraft, not the ground systems or the security of contractor information. GAO is conducting separate work evaluating the extent to which NASA has implemented information security controls that are in accordance with guidelines and standards, as well as leading cybersecurity practices.

To determine the extent to which NASA incorporated cybersecurity in spacecraft contracts, we selected three projects for our review by using GAO's 2020–2022 assessment of NASA major projects.[3] We selected these projects to represent different centers and stages of development and included both human space flight and robotic, or uncrewed, projects. The results are not generalizable to all NASA programs and projects. We identified relevant cybersecurity-related guidance—NASA's Space System Technical Standard—that is applicable to spacecraft acquisitions. We then analyzed contracts and related materials such as system specifications, risk management plans, and other documents to identify the extent to which NASA included requirements related to cybersecurity and the planned testing of those controls.

To determine the extent to which NASA determined whether additional cybersecurity updates, if any, are needed to its acquisition policies and standards for spacecraft, we first identified relevant NASA policies and standards related to spacecraft acquisition and any recent modifications. We interviewed officials with cybersecurity, contracting, engineering, and acquisition responsibilities as well as officials from the three selected spacecraft projects to discuss these policies and standards and any planned updates. We also reviewed NASA's *Space Security: Best Practices Guide* and interviewed officials who contributed to the development of the guide to understand the purpose, methodology, and future plans for implementation in NASA's policy or standards. We also determined that internal controls were significant to this review.[4]

[3] GAO, *NASA: Assessment of Major Projects*, GAO-20-405 (Washington, D.C.: Apr. 29, 2020); *NASA: Assessment of Major Projects*, GAO-21-306 (Washington, D.C.: May 20, 2021); and *NASA: Assessment of Major Projects*, GAO-22-105212 (Washington, D.C.: June 23, 2022).

[4] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

Specifically, we determined the control activities of federal standards for internal control were applicable to our objective. Appendix I contains detailed information on our objectives, scope, and methodology.

We conducted this performance audit from February 2023 to May 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Modern spacecraft depend on software and IT to achieve their intended performance. The growth of networked or internet-enabled technologies and devices in spacecraft heightens security risks in the face of increasingly sophisticated cyber threats from actors who have become capable of conducting damaging cyberattacks. Moreover, these malicious actors do not always need a great amount of skill to compromise IT systems because of the growing availability of public and commercial cyberattack tools.

Further, any exchange of information is a potential access point for an adversary. Spacecraft share information among various subsystems as well as with ground systems. A system designed and built to exchange information with many other systems or subsystems is more vulnerable to cyberattacks than a system without such connections. Therefore, it is vital to protect spacecraft from a malicious actor seeking to exploit a vulnerability in one of its subsystems or network and the resulting compromise of its confidentiality, integrity, or availability.

The consequences of malicious cyber activities include loss of mission data; decreased lifespan or capability of space systems or constellations; or the loss of positive control of space vehicles. One example involves a cyberattack on a satellite internet company in February 2022. Viasat, Inc. began experiencing outages with its European satellite internet service. These outages were triggered by an attacker running destructive commands against its network devices, according to Viasat.[5] A German wind turbine manufacturer reported that the attack affected remote operation of more than 5,000 turbines. Further, in August 2023, the

[5] GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, GAO-22-104256 (Washington, D.C.: Jun. 21, 2022).

National Counterintelligence and Security Center, the Federal Bureau of Investigation, and the Air Force Office of Special Investigations issued a warning about foreign entities seeking to disrupt or degrade satellites in operation and attempts to siphon intellectual property and other proprietary data from companies developing space technologies.[6]

The NASA Inspector General has also highlighted the importance of cyber preparedness noting that while attacks on NASA networks are not a new phenomenon, attempts to steal critical information are increasing in both complexity and severity. In 2018, the NASA Inspector General reported that NASA's Jet Propulsion Laboratory discovered an account belonging to an external user had been compromised and used to steal data from one of its major mission systems.[7] In 2021, the NASA Inspector General reported that NASA had experienced more than 6,000 cyberattacks over a 4 year period and was an attractive target for cyber criminals given its high-profile mission and relationship to the public, educational institutions, and other external organizations.[8]

System Requirements

System requirements are key performance parameters that must be in place before a system is operational. According to NASA policies, early in the acquisition life cycle, project officials use the system requirements process to identify what capabilities are needed and evaluate options to meet those needs while simultaneously protecting the system from cybersecurity threats. Security controls are then implemented as safeguards or countermeasures based on the requirements to protect the confidentiality, integrity, and availability of a system and its information. For example, a firewall is a common security control to allow or block information sent based on a set of rules.

Federal Cybersecurity Policy

In September 2020, the President issued Space Policy Directive–5. This directive establishes key cybersecurity principles to guide the cyber protection of space systems, which includes ground systems, sensor

[6] Office of the Director of National Intelligence's National Counterintelligence and Security Center, the Federal Bureau of Investigation, and Air Force Office of Special Investigations bulletin, *Safeguarding the U.S. Space Industry* (Washington, D.C.: Aug. 18, 2023).

[7] National Aeronautics and Space Administration, NASA Office of the Inspector General, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory,* IG-19-022 (Washington, D.C: June 18, 2019).

[8] National Aeronautics and Space Administration, NASA Office of the Inspector General, NASA's Cybersecurity Readiness*,* IG-21-19 (Washington, D.C: May 18, 2021).

networks, and one or more space vehicles.[9] The Policy Directive states that cybersecurity principles and practices that are used for ground systems also apply to space systems; encourages integrating cybersecurity into all phases of space systems development; and stresses that effective cybersecurity practices result from a culture of prevention, active defense, risk management, and the sharing of best practices. For example, one of the Policy Directive cybersecurity principles requires space vehicle developers to protect against unauthorized access to critical space vehicle functions. This includes safeguarding command, control, and telemetry links by using effective and validated authentication or encryption measures. It also directs U.S. government agencies to work with commercial companies to further define best practices, establish cybersecurity informed benchmarks, and promote improved cybersecurity behaviors in the U.S. industrial base for space systems.

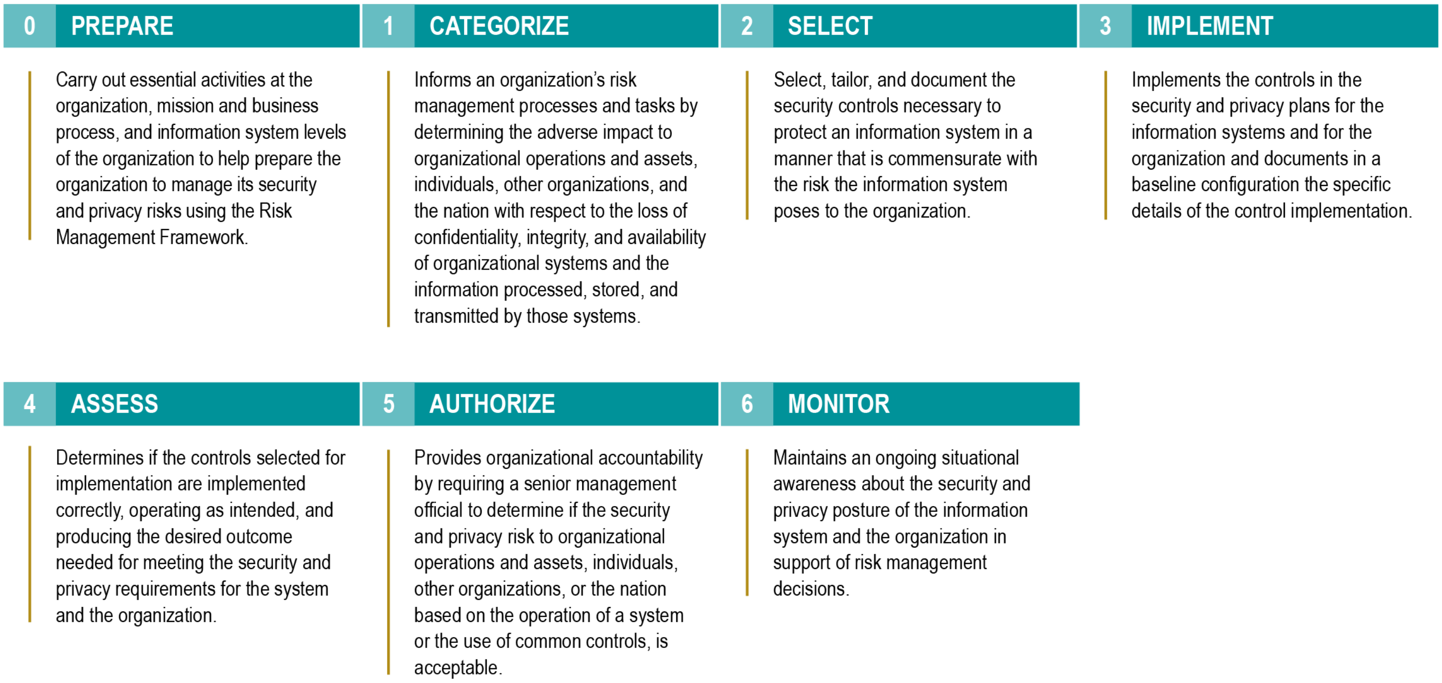
Government-wide Cybersecurity Standards and Guidance

The National Institute of Standards and Technology (NIST) has issued a suite of information security standards and guidelines that, collectively, provide comprehensive guidance on managing cybersecurity risks.

- **NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations (RMF).** NIST initially issued the RMF in 2010 in Revision 1 of Special Publication 800-37 and subsequently revised it in December 2018. The RMF includes a multistep process that provides organizations consistent NIST standards to manage cybersecurity risks. Specifically, the RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. Figure 1 shows the RMF steps.

[9] Space Policy Directive–5, 85 Fed. Reg. 56155 (Sept. 4, 2020).

Figure 1: Steps of National Institute of Standards and Technology's (NIST) Risk Management Framework



0 PREPARE

Carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.

1 CATEGORIZE

Informs an organization's risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

2 SELECT

Select, tailor, and document the security controls necessary to protect an information system in a manner that is commensurate with the risk the information system poses to the organization.

3 IMPLEMENT

Implements the controls in the security and privacy plans for the information systems and for the organization and documents in a baseline configuration the specific details of the control implementation.

4 ASSESS

Determines if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome needed for meeting the security and privacy requirements for the system and the organization.

5 AUTHORIZE

Provides organizational accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, other organizations, or the nation based on the operation of a system or the use of common controls, is acceptable.

6 MONITOR

Maintains an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

Source: GAO Analysis of NIST data. | GAO-24-106624

- **NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199).** In February 2004, NIST issued these standards, which define how agencies should determine the security category of their information and information systems. Agencies are to consider the potential impact or magnitude of harm that could occur should there be a loss in the confidentiality, integrity, or availability of the information or information system.
- **Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations.** In September 2020, NIST reissued this publication that establishes security and privacy control baselines for federal information systems and organizations. Organizations may use this catalog of controls, along with NIST-800-37, FIPS 199 and other NIST publications, as part of a risk-based control selection process to satisfy the security and privacy requirements in federal law and security standards. Federal agencies are required to implement security controls to protect federal information and information systems.

- **Special Publication 800-53A: Assessing Security and Privacy Controls in Information Systems and Organizations.** This NIST publication, reissued in January 2022, provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework, consistent with the controls in NIST Special Publication 800-53. The assessment procedures are executed at various phases of the system development life cycle. The procedures can be tailored to the needs of an organization. It also includes information on how to build assessment plans and guidance on analyzing assessment results.

NASA Enterprise Protection Program

The NASA Associate Administrator established the Enterprise Protection Program to focus on threats that may affect national security or that may affect a system critical to NASA or other federal agencies. The program is directed by the Principal Advisor for Enterprise Protection, who provides advice and recommendations on threats, vulnerabilities, mitigations to, and assessments of NASA missions and activities. However, the Principal Advisor for Enterprise Protection does not supplant the authorities or responsibilities of other officials in charge of protecting systems.

NASA Management of Space Flight and Information Technology Projects

The Office of the Chief Information Officer (OCIO) is responsible for planning, policy direction, and oversight for the management of NASA's IT, such as e-mail and communications systems, infrastructure, and administrative services. The OCIO is also responsible for ensuring compliance with the Federal Information Security Modernization Act of 2014 and conducting continuous monitoring activities for a variety of assets that heavily use IT. This includes mission ground infrastructure, such as, ground stations, mission operations centers, and science operation centers.[10] NASA Procedural Requirements (NPR) 7120.7, NASA Information Technology Program and Project Management Requirements, establishes requirements for these IT systems. NASA does not consider its spacecraft, or the IT incorporated within its spacecraft, to be IT systems that are subject to these requirements.

[10] The Federal Information Security Modernization Act *of 2014* (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). FISMA requires covered agencies, including NASA, to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their operations and assets. 44 U.S.C. § 3554(b).

The NASA Chief Program Management Officer (CPMO) provides policy direction, oversight, and assessment of the NASA space flight program and project management processes.[11] This includes the spacecraft acquisition process and the acquisition of the IT incorporated within the spacecraft. The CPMO is responsible for leading the agency-level program and project management integration function with support from other NASA organizations, including the Office of the Chief Engineer. The Chief Engineer is responsible for agency-level standards and policies as applied to engineering and program management, including cybersecurity for spacecraft.

NASA has defined procedural requirements—key decision points, project reviews, and roles and responsibilities—that establish the life-cycle requirements for different types of systems. Below are requirements and guidance that apply to the acquisition of all NASA space flight programs and projects.

- NPR 7120.5, NASA Space Flight Program and Project Management Requirements, establishes the process by which NASA formulates and implements space flight programs and projects. NASA's space flight programs and projects develop and operate a wide variety of spacecraft, launch vehicles, in-space facilities, communications networks, instruments, and supporting ground systems.[12] NPR 7120.5 also governs IT that is incorporated within these projects.
- NPR 7123.1, NASA Systems Engineering Processes and Requirements, establishes a systematic process and approach to developing, operating, maintaining, and disposing of systems throughout the life cycle of a project or program. NASA's systems engineering approach is intended to provide a standard set of processes that can be applied to different programs and projects regardless of the size, complexity, or type of program or project.

[11] NASA defines space flight programs and projects to include spacecraft, launch vehicles, instruments developed for space flight programs and projects, some research and technology programs and projects, technical facilities specifically developed or significantly modified for space flight systems, IT acquired as part of space flight programs and projects, and ground systems that are in direct support of space flight operations.

[12] Ground systems that are in direct support of space flight operations, such as mission operations centers, are also subject to NPR 2810.1, *Security of Information and Information Systems*, and its authorization process. NPR 2810.1 (Jan. 3, 2022).

In October 2019, the Chief Engineer issued a Space System Protection Standard that established agency-level protection requirements related to cybersecurity for all projects to address to ensure NASA missions are resilient to threats. These requirements include encrypting the communication between the ground and the spacecraft; protecting the positioning, navigation, and timing systems; and reporting any attempt to interfere with the spacecraft.[13] Subsequent NASA policy required this standard for all NASA programs and projects started after February 1, 2019.[14] NASA officials stated that they selected the requirements in the standard because they should be broadly applicable to all projects. Further, through the normal design process, individual projects should consider whether additional protections are required based on the needs and risks associated with the mission. NASA programs and projects that had already begun at the time the technical standard was issued were required to coordinate with the Office of the Chief Engineer to determine which requirements in the technical standard they should implement based on current malicious threat information. An example of a requirement in the technical standard related to cybersecurity includes encrypting communications between the ground and the spacecraft.

NASA's life-cycle requirements and engineering approach apply to systems that NASA builds as well as systems that it acquires from contractors. This means that NASA performs some activities and oversees the contractor's performance of other activities. NASA projects have different functional teams with expertise covering relevant areas of the system and oversee the contractor's work in their area, including cybersecurity.

Overview of Selected Spacecraft Projects

Gateway Power and Propulsion Element

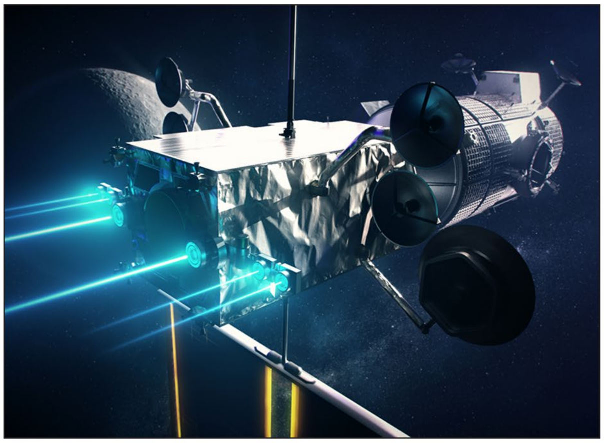
NASA is developing the Gateway Power and Propulsion Element (PPE) to provide power, communications, and the ability to change orbits, among other things to the Gateway—a sustainable outpost planned for lunar orbit. NASA plans to integrate the PPE and the Gateway's

[13] Positioning, navigation, and timing services are used in space for applications including real-time spacecraft navigation, timing, and scientific observations.

[14] National Aeronautics and Space Administration, NASA Procedural Requirements (NPR) 1058.1, *Enterprise Protection Program*, (June 14, 2019) (incorporating change 1, Jan. 19, 2021).

Habitation and Logistics Outpost (HALO) on the ground and launch them together. See figure 2 for an illustration of PPE.

Figure 2: Gateway Power and Propulsion Element



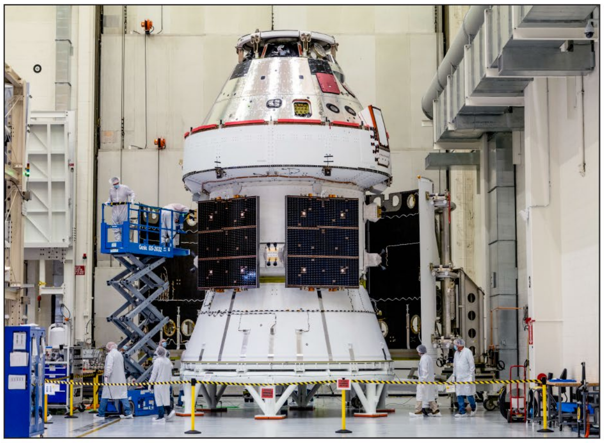
Source: NASA. | GAO-24-106624

In May 2019, NASA awarded a contract for the spacecraft design and build of PPE, and PPE is scheduled to launch with HALO no later than December 2027.

Orion Multi-Purpose Crew Vehicle

NASA is developing the Orion Multi-Purpose Crew Vehicle (Orion), as seen in figure 3, to transport and support astronauts beyond low-Earth orbit as part of the Artemis program. Orion will launch atop NASA's Space Launch System. The current design includes a crew module, service module, and launch abort system. Orion also includes the ability to conduct rendezvous proximity operations and docking. In November 2022, NASA conducted the Artemis I mission, which was the first test of an uncrewed Orion vehicle using the Space Launch System. The program is currently working to a September 2025 launch date for the Artemis II mission, its first crewed flight.

Figure 3: Orion Multi-Purpose Crew Vehicle



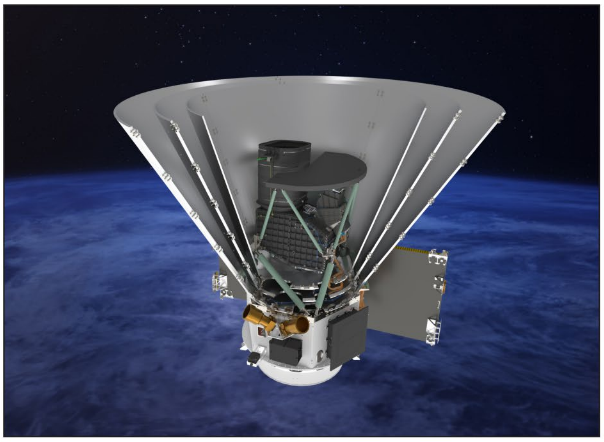
Source: NASA. | GAO-24-106624

NASA is currently integrating and testing the Orion Artemis II capsule, which will be used for the first crewed mission. In August 2006, NASA awarded a contract for Design, Development, Test, and Evaluation for the Exploration Flight Test 1, Artemis I, and Artemis II vehicles, including the formal human rated certification and first crewed flight.

Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer

NASA is developing the Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer (SPHEREx) mission to use a telescope to probe the origin and destiny of the universe, explore whether planets around the other stars could harbor life, and explore the origin and evolution of galaxies. The mission will create a map of the entire sky and survey the sky every 6 months to gather data on more than 450 million galaxies and 100 million stars in the Milky Way. See figure 4 for an illustration of SPHEREx.

Figure 4: Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer



Source: NASA/Jet Propulsion Laboratory-California Institute of Technology. | GAO-24-106624

NASA plans to launch SPHEREx no later than April 2025. The Jet Propulsion Laboratory, a federally funded research laboratory sponsored by NASA but operated by the California Institute of Technology, is developing and will operate SPHEREx.

Prior GAO Work

In March 2021, we reported that defining cybersecurity requirements within contracts was key to mitigate cybersecurity risk to systems at the Department of Defense (DOD).[15] Major systems contracts generally cover, among other things, the cost or price of the work to be performed, the schedule for delivering goods or services, and performance requirements. We found that, like other DOD system requirements, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met. Incorporating cybersecurity practices from the earliest stages of an acquisition is typically easier, less costly, and more effective than trying to add, or bolt on, cybersecurity protections late in the development cycle or after a system is fielded. When contractors have a key role in designing and building systems, the government must communicate its

[15] GAO, *Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*, GAO-21-179 (Washington, D.C.: Mar. 4, 2021).

cybersecurity requirements in its acquisition program contracts, just as it would with other types of performance requirements.

Selected NASA Spacecraft Contracts Require Contractors to Address NASA's 2019 Cybersecurity-Related Requirements

Each of the selected NASA spacecraft contracts included cybersecurity-related requirements, including that the contractors demonstrate that they satisfied these requirements, consistent with NASA's 2019 Space System Protection Standard.

Cybersecurity-related requirements. All three projects in our review—Orion, Gateway PPE, SPHEREx—were in development before NASA issued the Space System Protection Standard. NASA required such programs to coordinate with the Office of the Chief Engineer to determine whether any of the requirements should be incorporated based on threats.

Orion and Gateway PPE officials said that, following the release of the Space System Protection Standard, they reviewed their planned cybersecurity approach and determined their project's requirements aligned with those in the standard. The SPHEREx project protection plan indicated that the system requirements included all applicable requirements from the standard. Officials within the Office of the Chief Engineer agreed with the projects' assessment.

Our review of the contract and system specification documents for each of the selected projects confirmed that each of the projects either included requirements related to meeting the Space System Protection Standard objectives or planned to address the risk of the threat through another means. Table 1 includes an analysis of whether each selected project included protection requirements from the Space System Protection Standard.

Table 1: Selected Projects GAO Reviewed Included Protection Requirements from Space System Protection Standard (NASA-STD-1006)

Space System Protection Objectives	Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer	Orion Multi-Purpose Crew Vehicle	Gateway Power and Propulsion Element
Maintain command authority to prevent unauthorized access and to ensure data integrity	Not Applicable	Met	Met
Recognize and survive positioning, navigation, and timing (PNT) interference	Met	Met	Not Applicable
Detect and report unexplained interference	Met	Met	Met

Source: GAO analysis of National Aeronautics and Space Administration (NASA) data. | GAO-24-106624

Notes: All information is from system specification documents. There are a total of six space protection requirements within the three objectives. For example, the standard requires the command transmission to be protected with encryption.

In addition to addressing the Space System Protection Standard, there are additional examples of actions that projects took to address cybersecurity within the contract documents, such as:

- The Gateway PPE contract included a requirement for the system to use the space data link security protocol—a communication standard intended to provide a structured approach to implementing security for communication between satellites and ground systems.
- The Orion contract included a requirement that satellite control functions be isolated from other functions. Isolating system components from each other, also known as segmentation, is a common approach to strengthening cybersecurity as it may allow portions of a system to continue working properly even if other parts of the system are compromised. The National Security Agency and Cybersecurity and Infrastructure Security Agency (CISA) identified the lack of network segmentation as a common cybersecurity issue among large organizations.
- The SPHEREx contract included requirements to validate commands and reject invalid commands. This is a way to protect the spacecraft from malicious actors taking over the spacecraft, which may lead to loss of control resulting in damage, destruction, or loss of vehicle. CISA has identified numerous cybersecurity attacks that exploited improper input validation.

Testing. As we reported in 2018, cybersecurity controls must be properly designed and implemented to be effective, and testing is a better indicator of system security than system documentation.[16] Each of the selected projects require contractors to demonstrate that requirements have been implemented, operate as intended, and produced the desired outcome reflected in system security requirements. This is accomplished through a verification and validation process—a process to determine whether a project built the right system and whether that system was built correctly. For example, Gateway PPE's Verification and Validation Plan provides an overview of verification and validation activities planned for individual requirements and the system as a whole. The plan describes, among other things, how requirements will be verified (i.e., testing, analysis, demonstration, or inspection) and how the activities will be documented. The NASA verification and validation process covers the entire life cycle of a system from assessing potential vulnerabilities of the initial design to testing the final delivered software, including cybersecurity.

Responsibility for this process is typically shared among the contractors and the government. In addition, NASA has an Independent Verification and Validation program that helps ensure the software on NASA's highest-profile missions performs correctly. For example, teams from the Independent Verification and Validation Program performed verification and validation for the Orion program, providing support for both Artemis I and Artemis II. The team identified some cybersecurity-related issues pertaining to the Artemis I software design, including that the contractor did not address all cybersecurity-related requirements. Independent Verification and Validation program officials told us that these issues were either resolved or NASA chose to accept the risks. Further, these officials explained that while it is not their responsibility to make the decision to accept the risks—this determination is ultimately made by program officials—they were comfortable with the decisions made for Artemis I because it was an uncrewed test flight. The Independent Verification and Validation Program continues to provide support to Orion Project for Artemis II and the Gateway program, which includes PPE.

The three selected projects are at various stages of development and testing, and it is too soon to know the results of testing related to cybersecurity. For example,

[16] GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

- SPHEREx flight software is nearing the end of its development cycle and ongoing testing is scheduled to be completed no later than March 2024.
- Orion flight software testing for Artemis II—the first crewed launch—is ongoing and is expected to be completed in June 2024. As part of this testing, program officials stated that they have a joint Orion and contractor team that is developing a strategy based on a vulnerability assessment to identify specific cybersecurity risks, additional testing, and potential mitigations.
- Gateway PPE flight software is in the design and prototyping stages of development and it is too early to know when software testing will begin, according to project officials.

NASA Has Considered but Not Implemented Further Cybersecurity Updates to Its Spacecraft Acquisition Policies and Standards

Since the issuance of its 2019 set of cybersecurity requirements for projects to address, NASA has considered, but not yet implemented, updates to its spacecraft acquisition policies and standards. Specifically, in October 2023, NASA's Enterprise Protection Program released a Space Security: Best Practices Guide, in part, to further support the goals of Space Policy Directive 5, Cybersecurity Principles for Space Systems.[17] The guide contains information on cybersecurity principles and controls, threat actor capabilities, and potential mitigation strategies, among other things. With respect to principles and controls, NASA identifies three sets of security principles related to governance, space missions (including spacecraft), and ground systems.[18] For example, one space mission principle states that the mission should ensure only authenticated and authorized personnel, devices, and software are allowed to access the space system. The guide then describes how the principle applies to spacecraft and which NIST 800-53 controls are related to the principle.

In the guide, NASA notes it also serves the purpose of translating NIST language into spaceflight parlance. For example, the principles and controls in the guide relate to the government-wide cybersecurity guidelines that are captured in the Prepare and Select phases of the NIST RMF.

[17] National Aeronautics and Space Administration, *Space Security: Best Practices Guide*, Rev. B, (Jan. 19, 2024). NASA publicly released the first version of this guide on Dec. 22, 2023. Due to the timing of this review, we did not evaluate the contents of the guide.

[18] The term "space mission" in the best practices guide refers to a spacecraft, space-based hosted payload, or space-based infrastructure or architecture.

NASA spacecraft programs are encouraged to use the best practices guide but are not required to do so. NASA officials explained that they chose to issue a best practices guide—as opposed to formal technical requirements that can take a significant amount of time to adopt—because it offered the most timely way to share the information with the spaceflight community. They also explained that, due to the unique constraints of operating in space, NASA takes a cautious approach when introducing required changes to ensure feasibility because they do not have physical access to the spacecraft for repairs after launch.

NASA notes in the guide that the principles and controls will be evaluated for inclusion into agency standards and requirements. NASA officials stated that they plan to setup a cross functional team to inform further implementation, but they first want to receive feedback on the guide. However, officials did not have a timeline for implementation including when such an evaluation would be completed, what offices would be involved, or when any needed updates would happen.

NASA has a different approach for IT projects. In January 2022, NASA issued seven handbooks that provide new cybersecurity guidance for IT systems, including ground systems. NASA OCIO officials said that they did this to help unify multiple government cybersecurity laws and standards from the NIST RMF into handbooks for NASA officials.[19] According to NASA, the handbooks also serve as a mechanism to establish a common baseline of knowledge about each RMF step to inform a more uniform approach across the agency. Enterprise Protection Program officials explained that they had similar goals for the spacecraft best practices guidance. However, unlike the IT handbooks, which define NASA procedures to address NIST's RMF, NASA spacecraft programs are encouraged to use the best practices guide but are not required to do so.

Cybersecurity is a particularly dynamic environment in which threats and technology change rapidly. In addition to NASA indicating in the best practices guide that it plans to evaluate these practices for inclusion into policies and standards, *Standards for Internal Control in the Federal Government* states that management should periodically review policies, procedures, and related control activities for continued relevance and

[19] Subsequently, NASA updated the handbooks in June 2023. GAO has separate work that is evaluating NASA's IT policies, guidance, and implementation.

effectiveness in achieving an organization’s objectives or addressing related risks.[20]

Without establishing a plan to update its policies and standards to ensure they address essential cybersecurity controls in light of this dynamic environment, information in the guide remains optional for programs. As a result, NASA risks inconsistent consideration and implementation of cybersecurity controls and will not have full assurance that the spacecraft used to support NASA missions have a layered and comprehensive defense against cyberattacks.

Conclusions

Preventing, detecting, and responding to cyber threats are critical to NASA’s information systems and its spacecraft. Ensuring its spacecraft policies and standards incorporate guidelines that are foundational to effectively managing cybersecurity risks would enable NASA to make consistent, informed, risk-based decisions in the cybersecurity realm. While the contracts for spacecraft that we reviewed included requirements related to cybersecurity, it is important for NASA to ensure that cybersecurity practices are implemented consistently across spacecraft programs. NASA has taken some important steps in identifying how best to protect spacecraft from cyberattack. It is understandable that NASA must take a cautious approach to introducing cybersecurity changes that could affect spacecraft operations. However, NASA should balance this caution with being proactive given the dynamic and evolving nature of cyber threats. Ensuring updates to its spacecraft policies and standards are completed in a timely manner would provide NASA with greater confidence that its spacecraft are resilient to cybersecurity threats and reduce the risk of adverse consequences.

Recommendation for Executive Action

The NASA Administrator should ensure that the Chief Engineer, the Chief Information Officer, and the Principal Advisor for Enterprise Protection develop an implementation plan with time frames to update its spacecraft acquisition policies and standards to incorporate essential controls required to protect against cyber threats. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report to NASA for its review and comment. In written comments, reprinted in appendix II, NASA’s CIO partially concurred with the recommendation in the report. NASA also provided

[20] GAO-14-704G.

technical comments, which have been incorporated in the report, as appropriate.

Consistent with the recommendation, NASA agreed with the need to ensure continuous improvement of policies and standards, including those applicable to spacecraft acquisitions, to protect against cyber threats. However, NASA disagreed with the need to develop an implementation plan with time frames to update its spacecraft acquisition policies and standards against cyber threats. NASA's reasons for its disagreement and our responses follow below.

- **NASA's CIO said that it is not feasible to develop one set of essential controls applicable to all types of mission spacecraft and that the appropriate controls selection is performed by the program or project.**

  We did not suggest that NASA have one set of essential controls applicable to all spacecraft. Consistent with our recommendation, NASA should leverage its space security guide to determine the controls that address the likely threats to its spacecraft. NASA should subsequently incorporate these controls, as appropriate, into their policies or standards and allow spacecraft programs and projects to select those cybersecurity controls that are necessary to protect the systems.

- **NASA noted that transitioning traditional cybersecurity capabilities into a space environment requires careful consideration to avoid impacts to the spacecraft's objectives and the ability to operate safely.**

  We agree that cybersecurity controls must carefully be evaluated before inclusion into NASA agency standards and requirements. As we reported, in its space security guide, NASA expressed an intention to do such an evaluation. We think this would be a positive step, but without an implementation plan with time frames for doing so, NASA risks inconsistent consideration and implementation of cybersecurity controls in its missions.

- **NASA's CIO stated that NASA has an existing minimum re-validation schedule to ensure policy or standards remain appropriate for programs and projects.**

As we reported, cybersecurity is a particularly dynamic environment in which NASA should be proactive because the threats and technology change rapidly. For example, NASA issued a space security guide, as opposed to formal technical requirements, because it offered the timeliest way to share the information with the spaceflight community. However, NASA did not establish a timeline for further evaluation of which controls from the guide could be implemented into its policies or technical standards. Because the best practices listed in the space security guide are optional, NASA will not have full assurance that the spacecraft used to support its missions have a layered and comprehensive defense against cyberattacks. Consequently, we maintain that consistent with our recommendation, NASA should develop an implementation plan with time frames to update its spacecraft acquisition policies and standards to incorporate essential controls required to protect against cyber threats.

- **NASA said that the agency currently has existing policies and processes that evaluate risks and enable mission programs to select appropriate protection controls associated with its complex space systems.**

  While we do not dispute this, we note that NASA's space security guide recognizes that NASA does not currently have a cybersecurity risk management framework for end-to-end integrated space mission systems. The guide also notes that the identified best practices provide the beginning of an informed cybersecurity risk management framework specifically for spacecraft. Because of this, we maintain that NASA should develop an implementation plan to update its policies to incorporate these practices. In its comments, NASA agreed with the need to update its policies, but did not agree to set up a plan with dates to do so. Without a plan with identified timeframes, it is unknown when the agency will actually perform an update to incorporate, if necessary, any additional cybersecurity controls.

We believe implementing our recommendation to develop a plan to determine which additional security controls, if any, are needed would help ensure that NASA's spacecraft take into consideration the essential controls required to defend against cyberattacks. Furthermore, we believe that our recommendation remains valid and is aligned with the cybersecurity principles for space systems presented in Space Policy Directive–5.

We are sending copies of the report to the appropriate congressional committees and the NASA Administrator. In addition, the report will be available at no charge on GAO’s website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or RussellW@gao.gov or Kevin Walsh at (202) 512-6151 or WalshK@gao.gov. Contact points for our Offices of

Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

W. William Russell IV

W. William Russell
Director, Contracting and National Security Acquisitions

Kevin Walsh

Kevin C. Walsh
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Frank Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space and Technology
House of Representatives

The Honorable Brian Babin
Chairman
The Honorable Eric Sorensen
Ranking Member
Subcommittee on Space and Aeronautics
Committee on Science, Space and Technology
House of Representatives

The Honorable Donald S. Beyer, Jr.
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report assesses the extent to which the National Aeronautics and Space Administration (NASA) (1) incorporated cybersecurity in select spacecraft contracts and (2) determined whether additional cybersecurity updates, if any, are needed to its acquisition policies and standards for spacecraft.

For the first objective, we selected three projects to review. To select these projects, we first identified NASA projects with a life-cycle cost greater than $250 million, by using GAO's 2020–2022 assessment of NASA major projects.[1] We then intentionally selected three projects in order to account for projects that (1) were managed out of three different research centers, (2) covered different phases of development, and (3) included both a human space flight and uncrewed mission. After completing the steps above, we selected the projects in table 2.

Table 2: NASA Projects Selected for Review

Project	NASA Lead Center
Gateway Power and Propulsion Element	Glenn Research Center
Orion Multi-Purpose Crew Vehicle	Johnson Space Center
Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer	Jet Propulsion Laboratory

Source: GAO analysis of National Aeronautics and Space Administration (NASA) data. | GAO-24-106624

Although the results of our review of selected projects are not generalizable to all NASA programs and projects, the selected projects are intended to reflect the experiences and perspectives of projects from across NASA. This review focused on spacecraft, and not the ground systems or the security of contractor information.

For these three projects, we interviewed officials from the project offices and analyzed contracts and related materials including cybersecurity-related information in statements of work and system specifications. We compared this information with NASA's Space System Protection Standard. We also reviewed contract documents, such as the system specifications and statements of work, to determine if NASA included requirements related to cybersecurity that were not identified in this

[1] GAO, *NASA: Assessment of Major Projects*, GAO-20-405 (Washington, D.C.: Apr. 29, 2020); *NASA: Assessment of Major Projects*, GAO-21-306 (Washington, D.C.: May 20, 2021); and *NASA: Assessment of Major Projects*, GAO-22-105212 (Washington, D.C.: June 23, 2022).

standard. We also determined the extent to which contracts identify how NASA will verify that the contractor has satisfied these requirements.

For the second objective, we reviewed NASA policies, guidance, and standards related to the implementation of cybersecurity for spacecraft in development. These included

- NASA Procedural Requirements (NPR) 7120.5F, NASA Space Flight Program and Project Management Requirements;
- NASA Technical Standard, NASA-STD-1006, Space System Protection Standard;
- NASA Systems Engineering Handbook;
- NASA Space Flight Program and Project Management Handbook; and
- NASA Project Planning and Control Handbook.

We also reviewed Space Policy Directive-5. Finally, we reviewed NASA's October 2023 *Space Security: Best Practices Guide* to determine the scope and purpose of the guide. We compared information in the guide with the National Institute of Standards and Technology (NIST) Special Publication 800-37, Rev. 2: Risk Management Framework for Information Systems and Organizations to determine the extent to which information in the guide related to steps of the Risk Management Framework. We interviewed officials who contributed to the development of the guide to understand the purpose, methodology, and future plans for implementation in NASA's policy or standards.

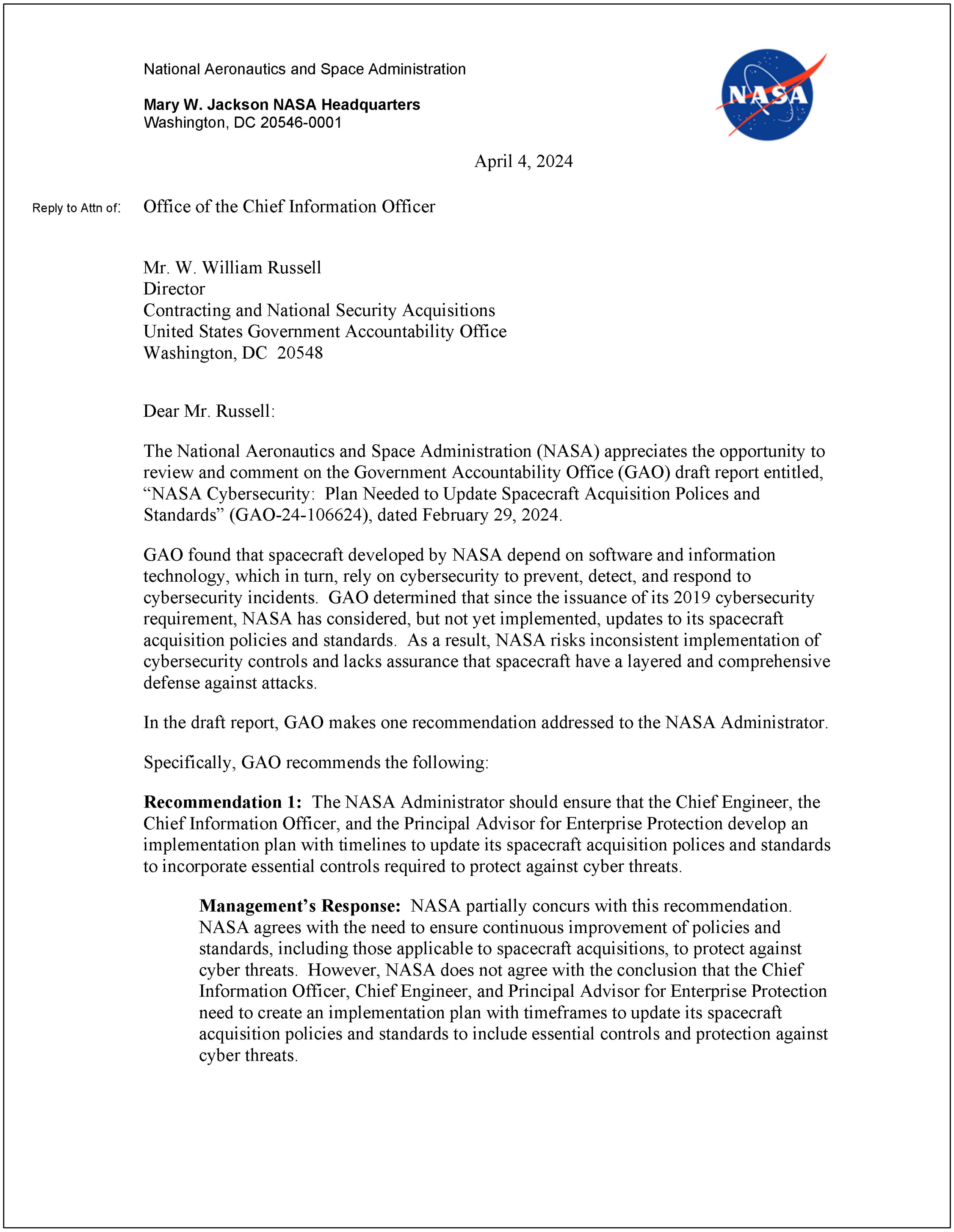
We also determined that internal controls were significant to the second objective.[2] Specifically, we determined the control activities of federal standards for internal control were applicable to our objective. To evaluate the principle that management should implement control activities through policies, we interviewed officials from Office of the Chief Information Officer and Office of the Chief Engineer to identify which policies related to the implementation of cybersecurity for spacecraft. We then reviewed those policies and compared to updates of other NASA policies and guidance that govern IT cybersecurity, including Information Technology Security Handbooks. We compared NASA's approach to

[2] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

updating policies for its IT programs with its plans to update policies and standards for spacecraft.

We conducted this performance audit from February 2023 to May 2024 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.

Appendix II: Comments from the National Aeronautics and Space Administration



National Aeronautics and Space Administration

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

April 4, 2024

Reply to Attn of: Office of the Chief Information Officer

Mr. W. William Russell
Director
Contracting and National Security Acquisitions
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Russell:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "NASA Cybersecurity: Plan Needed to Update Spacecraft Acquisition Polices and Standards" (GAO-24-106624), dated February 29, 2024.

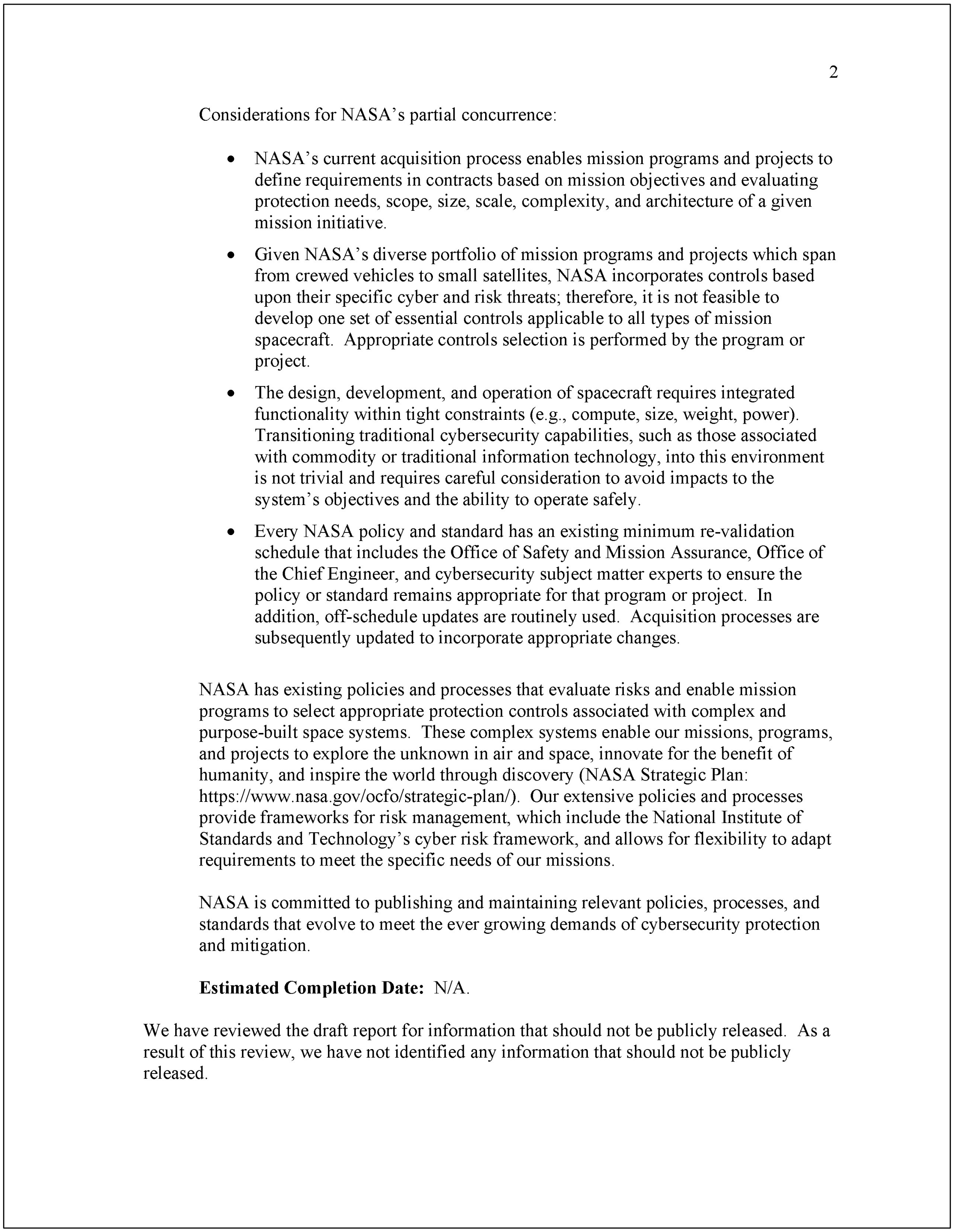
GAO found that spacecraft developed by NASA depend on software and information technology, which in turn, rely on cybersecurity to prevent, detect, and respond to cybersecurity incidents. GAO determined that since the issuance of its 2019 cybersecurity requirement, NASA has considered, but not yet implemented, updates to its spacecraft acquisition policies and standards. As a result, NASA risks inconsistent implementation of cybersecurity controls and lacks assurance that spacecraft have a layered and comprehensive defense against attacks.

In the draft report, GAO makes one recommendation addressed to the NASA Administrator.

Specifically, GAO recommends the following:

Recommendation 1: The NASA Administrator should ensure that the Chief Engineer, the Chief Information Officer, and the Principal Advisor for Enterprise Protection develop an implementation plan with timelines to update its spacecraft acquisition polices and standards to incorporate essential controls required to protect against cyber threats.

> **Management's Response:** NASA partially concurs with this recommendation. NASA agrees with the need to ensure continuous improvement of policies and standards, including those applicable to spacecraft acquisitions, to protect against cyber threats. However, NASA does not agree with the conclusion that the Chief Information Officer, Chief Engineer, and Principal Advisor for Enterprise Protection need to create an implementation plan with timeframes to update its spacecraft acquisition policies and standards to include essential controls and protection against cyber threats.



Considerations for NASA’s partial concurrence:

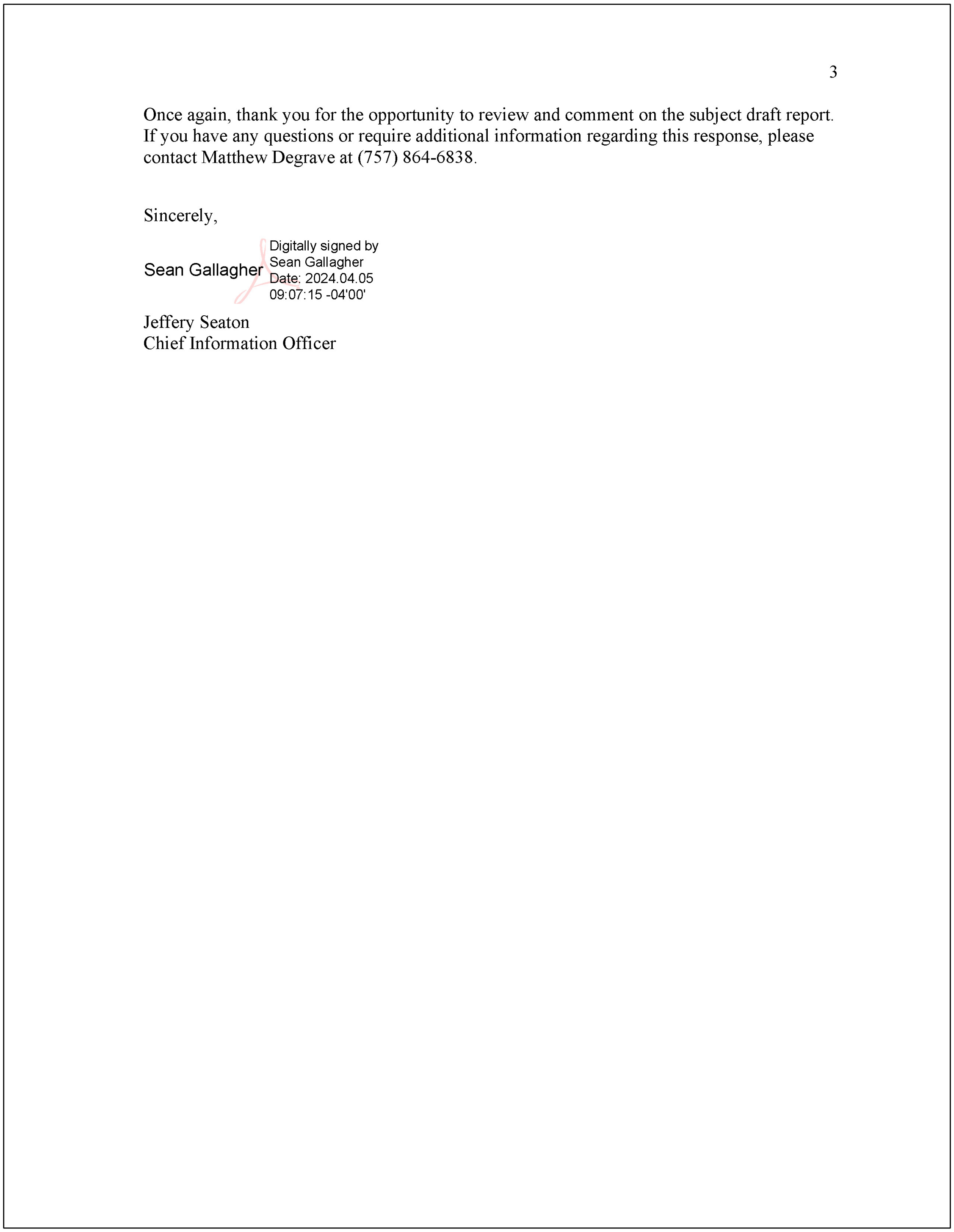
- NASA’s current acquisition process enables mission programs and projects to define requirements in contracts based on mission objectives and evaluating protection needs, scope, size, scale, complexity, and architecture of a given mission initiative.
- Given NASA’s diverse portfolio of mission programs and projects which span from crewed vehicles to small satellites, NASA incorporates controls based upon their specific cyber and risk threats; therefore, it is not feasible to develop one set of essential controls applicable to all types of mission spacecraft. Appropriate controls selection is performed by the program or project.
- The design, development, and operation of spacecraft requires integrated functionality within tight constraints (e.g., compute, size, weight, power). Transitioning traditional cybersecurity capabilities, such as those associated with commodity or traditional information technology, into this environment is not trivial and requires careful consideration to avoid impacts to the system’s objectives and the ability to operate safely.
- Every NASA policy and standard has an existing minimum re-validation schedule that includes the Office of Safety and Mission Assurance, Office of the Chief Engineer, and cybersecurity subject matter experts to ensure the policy or standard remains appropriate for that program or project. In addition, off-schedule updates are routinely used. Acquisition processes are subsequently updated to incorporate appropriate changes.

NASA has existing policies and processes that evaluate risks and enable mission programs to select appropriate protection controls associated with complex and purpose-built space systems. These complex systems enable our missions, programs, and projects to explore the unknown in air and space, innovate for the benefit of humanity, and inspire the world through discovery (NASA Strategic Plan: https://www.nasa.gov/ocfo/strategic-plan/). Our extensive policies and processes provide frameworks for risk management, which include the National Institute of Standards and Technology’s cyber risk framework, and allows for flexibility to adapt requirements to meet the specific needs of our missions.

NASA is committed to publishing and maintaining relevant policies, processes, and standards that evolve to meet the ever growing demands of cybersecurity protection and mitigation.

Estimated Completion Date: N/A.

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



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

Sincerely,

Sean Gallagher
Digitally signed by
Sean Gallagher
Date: 2024.04.05
09:07:15 -04'00'

Jeffery Seaton
Chief Information Officer

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

W. William Russell, (202) 512-4841 or RussellW@gao.gov, and Kevin C. Walsh, 202-512-6151 or WalshK@gao.gov.

Staff Acknowledgments

In addition to the contacts named above, Kathleen P. Sharkey (Assistant Director), Molly W. Traci (Assistant Director), Jose A. Ramos (Analyst in Charge), Peter Anderson, Brandon Booth, Dylan M. Desjardins, Joseph Shir, Andrew Stavisky, Anne Louise Taylor, Nathan A. Tranquilli, Shawn Ward, J. Andrew Walker, Alyssa Weir, and Adam Wolfe made significant contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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