CYBERSECURITY

NASA Needs to Fully Implement Risk Management

Report to Congressional Requesters

June 2025
GAO-25-108138
United States Government Accountability Office

Accessible Version

GAO Highlights

For more information, contact Kevin Walsh at walshk@gao.gov.

Highlights of GAO-25-108138, a report to congressional requesters

June 2025

CYBERSECURITY

NASA Needs to Fully Implement Risk Management

Why GAO Did This Study

NASA's space development project portfolio includes 36 major projects. Over the lifecycle of these projects, NASA plans to invest about $80 billion in them.

GAO was asked to review cybersecurity risk management at NASA. This report assesses the extent to which NASA implemented cybersecurity risk management for selected major projects.

GAO reviewed NASA policies and guidance regarding cybersecurity risk management. GAO selected a nongeneralizable sample of two major projects and two associated systems for each project. For the four selected systems, GAO analyzed system authorization documentation and compared it to seven key cybersecurity risk management steps and associated activities. GAO also interviewed project and cybersecurity officials.

This report is a public version of a sensitive report issued in March 2025. Information that NASA deemed sensitive has been omitted.

What GAO Recommends

GAO is making 16 recommendations to NASA to ensure that key activities within the risk management steps are being performed. These activities include (1) preparing and approving an organization-wide cybersecurity risk assessment, and (2) updating its guidance to help ensure that selected systems have documented continuous monitoring strategies. In its comments on the sensitive version of the report, NASA concurred with seven recommendations, partially concurred with four recommendations, and did not concur with the remaining five recommendations. GAO maintains that all recommendations are warranted.

This report is a public version of a "Controlled Unclassified Information" report issued in March 2025.

What GAO Found

Spacecraft and space systems are operating in a cyber threat environment with increased risks of attack and mission disruption. To help protect systems at federal agencies such as National Aeronautics and Space Administration (NASA), the National Institute of Standards and Technology developed cybersecurity risk management guidelines. The guidelines include seven key risk management steps: *prepare*, *categorize* systems, *select* controls, *implement* controls, *assess* control implementation, *authorize* the system, and continuously *monitor* security control effectiveness.

NASA fully or partially implemented all steps of its cybersecurity risk management program for selected systems. However, partial determinations indicate that NASA did not perform key activities within the steps. For example:

- For the *prepare* step, NASA did not have an approved organization-wide risk assessment. Such an assessment is essential to identifying and mitigating the highest priority cyber threats across the enterprise.
- Regarding the *monitor* step, selected systems did not document system-level continuous monitoring strategies due in large part to the lack of guidance on how to do so. Without documented strategies that are fully understood by key cyber personnel, organizations face increased risks of data breaches, delayed detection of threats, and slower responses to attacks.

The following table summarizes the extent to which NASA implemented each risk management step for the four selected systems.

Extent to Which National Aeronautics and Space Administration (NASA) and Selected Systems Implemented Risk Management Steps

Risk management step	Implementation by NASA organization
Prepare[a]	partially implemented

Risk management step	Implementation across selected systems
Categorize	partially implemented
Select	partially implemented
Implement	implemented
Assess	partially implemented
Authorize	partially implemented
Monitor	partially implemented

Legend: ●—implemented; ◐—partially implemented; ○—not implemented

Source: GAO analysis of NASA documentation. | GAO-25-108138

[a] For the review of the *Prepare* step, GAO evaluated the organizational-level activities and not the system-level activities.

Developing, implementing, and maintaining a comprehensive cybersecurity risk management program is critical to protecting NASA’s systems and information, detecting suspicious activity, and responding to incidents. Without a strong risk management program covering the selected systems, NASA faces increased risks that cyber incidents could result in loss of mission data, or decreased lifespan or capability of space systems.

Contents

Tables

Figures

Abbreviations

- CIO: Chief Information Officer
- CUI: controlled unclassified information
- FISMA: Federal Information Security Modernization Act of 2014
- NASA: National Aeronautics and Space Administration
- 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
- PPE: Power and Propulsion Element
- POA&M: plan of actions & milestones
- RMF: risk management framework
- RISCS: Risk Information Security Compliance System

June 25, 2025

Congressional Requesters

The National Aeronautics and Space Administration (NASA) depends on IT systems to develop, test, and operate its portfolio of 36 major mission projects. It plans to invest more than $81 billion over the lifecycle of these projects. 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, including command and control operational data and intellectual property on the design of the spacecraft. The security of the systems supporting these projects is vital because of the risks if such data are stolen or manipulated.

Cyber-based threats to sensitive data associated with NASA's major mission projects are becoming increasingly prevalent. NASA leverages a large network of interconnected IT systems and data, including sensitive and proprietary data, to achieve its mission. Because of NASA's high-profile mission, complex IT infrastructure, and large number of partnerships, it is important that NASA takes actions to adequately protect its systems and sensitive data.

You asked us to conduct a review of the cybersecurity risks to the sensitive data associated with NASA's major projects and spaceflight operations. Our specific objective was to assess to what extent NASA implemented a cybersecurity risk management program for selected major projects. We are also conducting separate work evaluating the extent to which NASA effectively implemented cybersecurity controls for selected mission critical systems.

In March 2025, we issued a report that assessed the extent that NASA had implemented a cybersecurity risk management program for selected major projects.[1] In the report, we made 16 recommendations to NASA to ensure that key activities within seven cybersecurity risk management steps are being performed. We designated that report as "controlled unclassified information" (CUI) and did not release it to the general public because of the sensitive information it contained.

This subsequent report publishes the findings discussed in our March 2025 report, but we have removed all references to the sensitive information. Specifically, we deleted the names of the systems that we examined and omitted details from our findings associated with NASA's implementation of key cybersecurity control assessment activities. Additionally, we omitted tables summarizing system-specific findings throughout the report. Although the information provided in this report is more limited, it addresses the same objectives as the sensitive report and uses the same methodology.

[1] GAO, *Cybersecurity: NASA Needs to Fully Implement Risk Management*, GAO-25-105882SU (Washington, D.C.: Mar. 12, 2025).

As noted in our CUI report, to accomplish our objective, we selected two projects to be in the scope of our review by using assessments of NASA major projects we performed from 2020 to 2022.[2] We selected these projects to ensure coverage of different facilities and different stages of development.

Based on these criteria, we selected the following projects:

- Gateway Power and Propulsion Element (PPE)
- Orion Multi-Purpose Crew Vehicle

We then selected two IT systems that were used by each of these projects and that process, store, and transmit sensitive data.[3] To assess the four systems, we identified key cybersecurity risk management steps and supporting activities consistent with selected leading practices from the National Institute of Standards and Technology (NIST) and NASA's risk management policies, procedures, and guidance. We reviewed and analyzed agency documentation that was part of the most recently approved authorization package for each system at the time of our review, including system security plans and security assessment reports.[4] We also reviewed exports from NASA's data repository for cybersecurity-related system information.

In addition, we analyzed updated system documentation that had been developed after the authorization packages had been approved, and updated our analyses based on this information as necessary. We made determinations based on the documents and data provided about the extent to which officials for each system implemented the identified key activities for each risk management step.

We rated NASA's actions as "implemented" if NASA provided complete evidence that satisfies the entire selected criterion; "partially implemented" if NASA provided evidence that satisfies some but not all of the selected criterion; and "not implemented" if NASA provided no evidence that satisfies any of the selected criterion. The results of our analyses are not generalizable to all NASA programs, projects, and systems.

We also provided a draft of this report to NASA officials to review and comment on the sensitivity of the information. These officials affirmed that the report can be made available to the public without jeopardizing the security of NASA's information systems and networks. Appendix I contains detailed information on our objective, scope, and methodology.

The performance audit upon which this report is based was conducted from March 2022 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

[2] 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).

[3] The two selected projects use the selected systems, but do not own or manage them.

[4] An authorization package is the essential information that an authorizing official uses to determine whether to authorize the operation of an information system. The authorization package includes an executive summary, system security plan, security control assessment, and any relevant plans of action and milestones.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with NASA from February 2025 to June 2025 to prepare this version of the original CUI report for public release. This public version was also prepared in accordance with these standards.

Background

NASA is America's civil space program and global leader in space exploration. It develops and funds space technologies that will enable future exploration. For example, NASA's Exploration Systems Development Mission Directorate leads a Moon to Mars exploration approach, which includes working with U.S. industry, international partners, and academia to develop new technology. This Moon to Mars approach is expected to send science research, and soon humans, to explore the Moon on Artemis missions.

Modern spacecraft depend on software and IT to achieve their intended performance. However, these spacecraft face heightened security risks because they rely on networked or internet-enabled technologies and devices, and because cyberattacks from threat actors are becoming increasingly sophisticated. Moreover, these malicious actors may be able to leverage the growing availability of public and commercial cyberattack tools.

The consequences of malicious cyber activities can include loss of mission data, decreased lifespan or capability of space systems or constellations, or the loss of positive control of space vehicles. For example, in February 2022, a satellite internet company—Viasat, Inc.—suffered a cyberattack. The company began experiencing outages with its European satellite internet service. According to Viasat, these outages were triggered by an attacker running destructive commands against its network devices.[5] Further, in August 2023, the 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]

NASA's 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. For example, in 2018, the NASA's Office of Inspector General (OIG) 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 addition, in 2021, NASA's OIG 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 relationships to the public, educational institutions,

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

[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).

and other external organizations.[8] Further in 2023, NASA's OIG reported that the agency's Office of the Chief Information Officer (OCIO) security systems blocked 5 billion attempts per day of malicious and unauthorized network traffic, including approximately 1.5 million email threats per week.[9]

Role of NASA's Chief Information Officer

For fiscal year 2023, NASA's IT budget was roughly $2.2 billion; the OCIO manages $667 million of the $2.2 billion.[10] NASA's OCIO centrally manages the enterprise IT that centers and mission directorates leverage to conduct and protect their missions and projects.

NASA's Chief Information Officer (CIO) is responsible for providing leadership, planning, policy direction, and oversight for the management of the agency's information and systems, including email and communications systems, infrastructure, and administrative services. In addition, the CIO is expected to report directly to the NASA Administrator and serves as the principal advisor to the Administrator and senior officials on all matters pertaining to IT.

The CIO is also responsible for ensuring compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and conducting continuous monitoring activities for a variety of assets that heavily use IT.[11] This includes mission ground infrastructure, such as ground stations, mission operations centers, and science operation centers.

Finally, the CIO is responsible for developing and updating agency-wide information security policies and processes. Specifically, NASA Procedural Requirement 2810 requires the CIO to develop and maintain an information security program.[12] This includes publishing and maintaining information security handbooks to provide detailed information regarding NASA's processes to meet its information security program requirements.

Cybersecurity Risk Management

Cybersecurity risk management comprises a full range of activities undertaken to protect IT systems and data from cyber threats such as unauthorized access. This involves maintaining awareness of these threats, as well

[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).

[9] National Aeronautics and Space Administration, NASA Office of the Inspector General, *NASA's Top Management and Performance Challenges*, (Washington, D.C.: November 2023).

[10] A portion of the IT budget is controlled by mission directorates.

[11] The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). The act 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).

[12] National Aeronautics and Space Administration, NASA Procedural Requirements 2810.1F, *Security of Information and Information Systems*, (Jan. 3, 2022).

as detecting anomalies and incidents adversely affecting IT systems and data. Additionally, risk management includes responding to and recovering from cybersecurity incidents and mitigating their impact.

Federal law and guidance specify requirements for protecting federal information and information systems, including space systems. Specifically, FISMA requires agencies to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their mission.[13]

In addition, the Office of Management and Budget's (OMB) Circular A-130 establishes minimum requirements for federal information security programs and assigns federal agency responsibilities for the security of information systems.[14] It requires federal agencies to develop and implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security on an ongoing basis across the organization. It also requires agencies to implement a risk management framework to guide and inform the categorization of federal information and information systems; the selection, implementation, and assessment of security controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.

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 networks, and one or more space vehicles.[15] The directive also 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 best practice sharing.

NIST's Government-wide Cybersecurity Standards and Guidance

NIST was tasked with developing standards and guidelines for agencies to use in establishing minimum cybersecurity requirements for such information and information systems based on their respective levels of cybersecurity risk.[16] 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).**[17] In December 2018, NIST issued NIST 800-37. The RMF includes a multistep process that provides organizations consistent standards to manage cybersecurity risks. It also 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

[13] 44 U.S.C. § 3554(b). The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014), updated and largely superseded the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (2002). As used in this report, the Federal Information Security Modernization Act refers to the requirements in the 2014 law and the relevant requirements from the 2002 law that were unchanged by the 2014 law and continue in full force and effect.

[14] Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (July 28, 2016).

[15] Space Policy Directive-5, *Cybersecurity Principles for Space Systems*, 85 Fed. Reg. 56155 (Sept. 4, 2020).

[16] 15 U.S.C. § 278g-3(a)-(b).

[17] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, revision 2 (Gaithersburg, MD: Dec. 2018).

authorizations; and continuous monitoring. Table 1 describes the steps of NIST's RMF, along with a summary of key activities for each step.

Table 1: Description of Risk Management Framework (RMF) Steps and Summary of Key Activities for Each Step

RMF steps	Step description	Summary of key activities
Prepare (organizational-level)[a]	To carry out essential activities at the organization (or department), mission (or bureau), and information system levels of the organization to help prepare to manage its security risks using the RMF.	Assign security and privacy risk management roles and responsibilities. Establish and document an organizational-wide risk management strategy. Assess organization-wide security and privacy risk. Identify common security controls. Implement an organization-wide strategy for continuously monitoring control effectiveness.
Categorize	To guide and inform risk management processes, systems are categorized to identify potential impact of loss.	Develop system description. Categorize systems based on risk. Review and approve system security categorization.
Select	Identify security controls based on the system categorization performed in step one and tailor the controls as needed to reduce risk to an acceptable level.	Select control baselines. Tailor controls. Document planned control implementation. Plan review and approval.
Implement	Describe and implement the controls within the system.	Implement controls and document the details of the implementation.
Assess	Determine if selected controls are implemented and operating correctly with respect to satisfying the security and privacy requirements.	Evaluate the implementation of selected controls and document the results. Prepare security assessment reports. Address control deficiencies by developing plans of action and milestones for controls that cannot be immediately addressed.
Authorize	Review all system security related documentation to determine to either grant or deny an authorization to operate.	Create an authorization package. Conduct a risk analysis. Evaluate the risk response actions taken. Make a decision to approve or deny the authorization. Document the decision.
Monitor	Develop and document a system-level strategy for continuous monitoring of security control effectiveness.	Conduct ongoing assessments of control effectiveness in accordance with an established continuous monitoring strategy. Identify, analyze, and respond to risks on an ongoing basis. Update risk management documents based on the continuous monitoring process.

Source: GAO analysis of National Institute of Standards and Technology. | GAO-25-108138

[a] For this review, we evaluated the organizational-level activities and not the system-level activities of the prepare step.

- **NIST Federal Information Processing Standards Publication 199 (FIPS Pub 199): Standards for Security Categorization of Federal Information and Information Systems.**[18] In February 2004, NIST issued FIPS Pub 199, which defines 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.

[18] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: Feb. 2004).

- **NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations.**[19] In September 2020, NIST reissued NIST 800-53 which 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 Pub 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.
- **NIST Special Publication 800-53A: Assessing Security and Privacy Controls in Information Systems and Organizations.**[20] 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 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 Cybersecurity Risk Management Policies

NASA has documented its policies and procedures for cybersecurity risk management in its IT security handbooks, which were prepared following NIST guidance. The handbooks are intended to supplement and place a NASA-specific perspective on the seven RMF steps. In general, these handbooks outline the policies and procedures for documenting, assessing, remediating, and reporting on NASA's cybersecurity posture and addressing the agency's cybersecurity objectives.

NASA's implementation of the RMF is supported by the agency's Risk Information Security Compliance System (RISCS). RISCS is a data repository and tool that is intended to collect, store, and manage supporting documentation and reports associated with the RMF and NASA's associated cybersecurity risk management policies. This includes system security plans, security assessment reports, plans of actions and milestones (POA&M), and documentation related to risk-based decisions and authorizations to operate.

Overview of Selected Spacecraft Projects

Gateway Power and Propulsion Element

NASA is developing the Gateway PPE to provide power, communications, and the ability to change orbits, among other things, to the Gateway program. Gateway is a program comprised of multiple projects to build a sustainable outpost planned for lunar orbit that will serve as a staging point for human exploration in deep space. NASA plans to integrate the PPE and the Gateway's Habitation and Logistics Outpost on the ground and launch them together.[21] In May 2019, NASA awarded a contract for the spacecraft design and build of

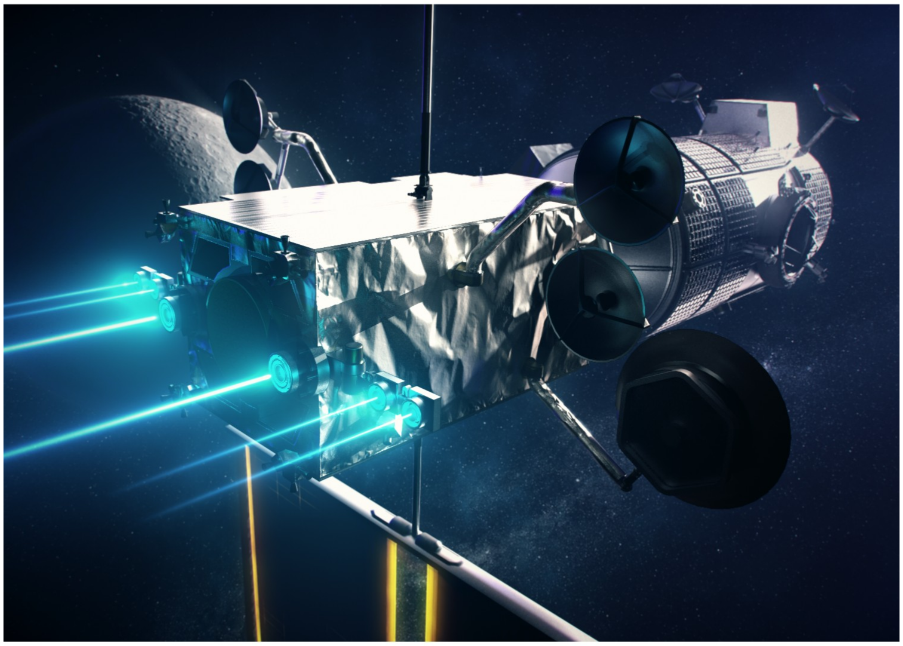
[19] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: Sept. 2020).

[20] National Institute of Standards and Technology, *Assessing Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53A, revision 5 (Gaithersburg, MD: Jan. 2022).

[21] Gateway's Habitation and Logistics Outpost is the initial crew module for the Gateway program and will provide living quarters and communication functions to the lunar surface.

PPE. PPE is scheduled to launch with the Habitation and Logistics Outpost no later than December 2027. See figure 1 for an illustration of PPE.

Figure 1: Gateway Power and Propulsion Element



Source: National Aeronautics and Space Administration (image). | GAO-25-108138

The Gateway-PPE project uses several IT systems to store, process, or transmit design and development specifications, including two of the selected systems in our review.[22]

Orion Multi-Purpose Crew Vehicle

NASA is developing the Orion Multi-Purpose Crew Vehicle (Orion), as seen in figure 2, to transport and support astronauts beyond low-Earth orbit as part of the Artemis program. 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 December 2022, NASA completed the first test of an uncrewed Orion vehicle as part of the Artemis I mission. The program is working toward a scheduled 2026 launch date for the Artemis II mission, which is intended to include Orion.

[22] Specific details about the selected systems were omitted because this information is considered sensitive.

Figure 2: Orion Multi-Purpose Crew Vehicle

Source: National Aeronautics and Space Administration (image). | GAO-25-108138

The Orion program uses several IT systems to store, process, or transmit command and control operational data through the Flight Operations Directorate at Johnson Space Center, including two of the selected systems in our review.[23]

GAO and Others Have Reported on Challenges in NASA's Cybersecurity Risk Management

Along with NASA's OIG, we have issued reports in recent years that discussed challenges NASA has faced related to cybersecurity risk management. For example:

- In May 2024, we reported that NASA had issued a space best practices guide containing information on cybersecurity principles and controls, threat actor capabilities, and potential mitigation strategies, among other things.[24] However, NASA did not have an implementation plan and time frame to incorporate additional security controls into acquisition policies and standards. We recommended that NASA 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 partially concurred with the recommendation, and as of May 2025, it has not been implemented.
- In November 2023, NASA's OIG reported that the agency's OCIO had begun consolidating assessment and authorization activities, reducing duplication, and standardizing cybersecurity services for institutional

[23] Specific details about the selected systems were omitted because this information is considered sensitive.

[24] GAO, *NASA Cybersecurity: Plan Needed to Update Spacecraft Acquisition Policies and Standards*, GAO-24-106624 (Washington, D.C.: May 1, 2024).

and mission systems.[25] NASA's OIG noted that the agency is likely years away from an enterprise approach to IT management due to the current decentralized approach. NASA's OIG also reported that the decentralized management structure negatively affected the agency's ability to protect information and IT systems vital to its mission.

- In its annual FISMA report published in August 2023, NASA's OIG found that the agency's information security program and practices were not effective.[26] Among other things, NASA's OIG found that the information security continuous monitoring strategy did not follow federal cybersecurity guidance. It also reported NASA did not have accurate, complete, and up-to-date cybersecurity risk management information for selected systems. In addition, it reported that NASA did not update and approve POA&Ms—which are corrective action plans that document planned actions to correct weaknesses or deficiencies—in a timely manner. These findings were consistent with NASA OIG's annual report from 2022, which also found that two of NASA's selected systems did not update information related to systems' authorization to operate on a continuous or annual basis.[27]
- In May 2018, we reported that NASA had not fully established an effective approach to managing agency-wide cybersecurity risk.[28] Among other things, we found that NASA had not yet established an agency-wide cybersecurity risk management strategy. Thus, we recommended that NASA establish an agency-wide approach to managing cybersecurity risk that includes a cybersecurity strategy. Such a strategy should, among other things, describe the agency's risk tolerance, accepted risk assessment methodologies, a process for consistently evaluating risk across the organization, response strategies and approaches for monitoring risk over time, and priorities for risk management investments. NASA concurred and implemented this recommendation by establishing and finalizing the strategy in May 2024.

NASA Did Not Fully Implement Cybersecurity Risk Management Program for Selected Projects

We reported in March 2025 that NASA had not fully implemented its cybersecurity risk management program for selected projects and associated systems. Specifically, of the seven RMF steps, the implement step was fully implemented by all four selected systems, the categorize step was fully implemented by three selected systems, and the remaining steps were partially implemented. Table 2 summarizes the extent to which NASA implemented each risk management step for the four selected systems.

[25] National Aeronautics and Space Administration, *NASA's Top Management and Performance Challenges*, (Washington, D.C.: November 2023).

[26] National Aeronautics and Space Administration, NASA Office of the Inspector General, *NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023*, IG-23-017 (Washington, D.C.: Aug. 17, 2023).

[27] National Aeronautics and Space Administration, NASA Office of the Inspector General, *NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022*, IG-23-006 (Washington, D.C.: Dec. 19, 2022).

[28] GAO, *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, GAO-18-337 (Washington, D.C.: May 22, 2018).

Table 2: Extent to Which National Aeronautics and Space Administration (NASA) and Selected Systems Implemented Risk Management Framework (RMF) Steps

RMF steps	Implementation by NASA organization
Prepare[a]	partially implemented

RMF steps	Implementation across selected systems
Categorize	partially implemented
Select	partially implemented
Implement	implemented
Assess	partially implemented
Authorize	partially implemented
Monitor	partially implemented

Legend: ●—implemented; ◐—partially implemented; ○—not implemented

Source: GAO analysis of NASA documentation. | GAO-25-108138

[a] For the review of the Prepare step, GAO evaluated the organizational-level activities and not the system-level activities.

The purpose of the ***prepare*** step in the NIST Risk Management Framework is to ensure that an organization is ready to carry out essential activities at the organizational level to help prepare the organization to manage its security risks.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-25-108138

NASA Partially Implemented Key Activities for Preparing the Agency to Manage Cybersecurity Risks

The *prepare* step includes five key activities carried out at the organization level. These preparatory tasks support all subsequent risk management activities.

Of the five key activities, NASA fully implemented three, partially implemented one, and did not implement one. Table 3 summarizes our assessment of the extent to which NASA implemented each task in the *prepare* step of the NIST RMF at the organization level.

Table 3: Extent to Which National Aeronautics and Space Administration (NASA) Implemented Key Activities in the Prepare Step of the Risk Management Framework at the Organization Level

Key activities in the prepare step	GAO assessment	Summary of assessment
Risk management roles: identify and assign individuals key roles for executing the risk management framework.	implemented	NASA identified and assigned individuals to specific roles associated with security and privacy risk management and ensured that these individuals have the proper authority to perform their role.
Risk management strategy: establish an organization-wide risk management strategy that includes a determination and expression of organizational risk tolerance.	implemented	NASA approved an organizational cybersecurity risk management strategy in May 2024.
Risk assessment: complete an organization-wide risk assessment or update an existing risk assessment. The organization-wide risk assessment leverages aggregated information from system-level risk assessment results, continuous monitoring, and any strategic cybersecurity risk considerations relevant to the organization.	not implemented	NASA officials stated the agency does not have an approved organization-wide risk assessment.
Common control identification: identify, document, and publish common controls that are available for inheritance by organizational systems.	implemented	NASA identified and documented common controls that are available for inheritance by NASA's systems.
Continuous monitoring strategy: develop and implement an organization-wide strategy for monitoring control.	partially implemented	NASA provided an undated organization-wide strategy for continuously monitoring control effectiveness. NASA intends to develop an implementation plan for the continuous monitoring strategy, which is expected to include major activities and milestones for implementing it. However, in August 2023, NASA's OIG made a series of recommendations for the agency to update its strategy to align with federal cybersecurity guidance.[a] As of May 2025, NASA's OIG reported the recommendations remained open.

Legend: ●—implemented; ◐—partially implemented; ○—not implemented

Source: GAO analysis of NASA documentation. | GAO-25-108138

[a] National Aeronautics and Space Administration, NASA Office of the Inspector General, *NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023*, IG-23-017 (Washington, D.C.: Aug. 17, 2023).

NASA officials stated the agency does not have an approved documented organization-wide risk assessment. Instead of completing and documenting the results of such an assessment, officials stated that NASA's OCIO provides cybersecurity risk management oversight in various ways. These include developing a cybersecurity risk management strategy, performing information security continuous monitoring, maintaining current threat information, compiling system-level security risk assessment results, and managing supply chain risks.

However, a documented organization-wide risk assessment is essential to identifying and mitigating the highest priority cyber threats across the enterprise. Without such an assessment, NASA is less likely to be in the position to identify relevant threats and internal and external vulnerabilities, determine the impact if these threats and vulnerabilities are exploited, and ascertain the likelihood that harm will occur.

Regarding the continuous monitoring strategy, as mentioned in the table, NASA's OIG made recommendations that the agency update its strategy to align with federal cybersecurity guidance. If NASA addressed these recommendations, it would be better positioned to fully manage its security risks.

NASA Partially Implemented Activities to Categorize Security Levels

By ***categorizing systems***, programs determine the extent to which threats could adversely impact the organization and the extent to which systems are vulnerable to these circumstances or events.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-25-108138

As part of the *categorize* step, NIST and NASA guidance require system owners to implement three key activities:

- **Develop system descriptions.** System descriptions ensure that stakeholders understand the purpose and functions of the system and its components. They should include the intended users and the intended uses of the data that each system processes, stores, and transmits.
- **Categorize systems based on risk.** The system's information security officer is to identify the types of data expected to be processed, stored, and transmitted by the system. Based on the information types identified, NASA's RISCS automatically selects a provisional impact level (low, moderate, or high) for the system in the areas of confidentiality, integrity, and availability.[29] The security officer then is to review the provisional impact level for these areas, determine whether any need to be modified, select security categorization levels (low, moderate, high) in those areas based on the provisional impact levels and other information, and document the results in RISCS. In cases where the information security officer modifies a provisional impact level, NASA guidance requires that they provide sufficient justification for that change. Once these impact levels are finalized, the security officer is to determine the overall security categorization (low, moderate, or high) of the system.
- **Review and approve system security categorization.** Categorization results are to be documented and subsequently reviewed and approved by senior officials (including the system's Chief Information Security Officer and authorizing official).

NASA fully implemented the three activities in the *categorize* step for three of the four selected systems. NASA also fully implemented two of the three activities for the remaining selected system, and partially implemented the third activity.

For each of the four selected systems, NASA officials fully developed system descriptions that included information on the intended users of the system and the intended uses of the data that the system processes, stores, and transmits. In addition, after system categorization, senior officials for each selected system (including the system's Chief Information Security Officer and authorizing official) reviewed and approved the impact levels.

NASA also took steps to categorize selected systems based on risk. For example, the systems' Chief Information Security Officers identified the types of data expected to be processed, stored, and transmitted by each system. Based on this information, RISCS automatically assigned provisional impact levels for each of the four selected systems in the areas of confidentiality, integrity, and availability based on the identified information types. After reviewing the assigned provisional impact levels, the information security officers for two of the four selected systems made changes to those impact levels within RISCS, which is permitted by NASA policy as long as a rationale is documented. Officials for one of these two systems documented a

[29] NASA uses RISCS to record and manage cybersecurity-related documentation (including documentation for each of the RMF steps). After an information security officer identifies the information types, this cybersecurity risk management tool automatically generates provisional impact levels for NASA's systems based on the impact levels for each of the information types that are identified.

rationale for the change to the impact level as required by NASA policy, but officials for the other system did not.

In addition, officials for one of the systems inconsistently documented the security categorization impact levels for the confidentiality and integrity of the system. Specifically, the impact levels documented within RISCS as of March 2024 conflict with the related security assessment report as well as impact levels presented to the authorizing official.

Officials for this system acknowledged that the impact levels entered into RISCS were not accurate and were unsure about the cause of the inaccuracies. These officials stated that they would ensure that the information documented in RISCS was updated to be consistent with what was presented to the authorizing official. They noted that, even with the disparate impact levels among the documentation, the overall security categorization of the system was correct according to NASA policy even though the underlying impact levels were not.

Nevertheless, the identified inaccuracies in the system security categorization within RISCS call into question whether NASA officials are ensuring that information in RISCS is of good quality (i.e., appropriate, current, complete, and accurate). Moreover, until NASA ensures that RISCS includes accurate impact levels for its systems, the agency risks either over-protecting systems (wasting valuable resources), or under-protecting systems (placing important operations and assets at risk).

NASA Implemented Key Activities of Control Selection but Did Not Fully Apply Proper Control Baselines for Selected Systems

To select controls for each system, NIST and NASA guidance require each system to implement four key activities:

Building upon the system categorization, the ***select*** step has NASA system owners select, tailor, and document the security controls necessary to protect an information system and NASA in a manner that is commensurate with the risk the system poses to the organization.

Source: GAO analysis of National Institute of Standards and Technology and National Aeronautics and Space Administration information. | GAO-25-108138

- **Select and apply a control baseline based on the security categorization.**[30] Once a system categorization is approved as part of the *categorize* step, a corresponding control baseline is automatically selected by RISCS. For example, systems categorized as moderate impact are assigned a moderate IT baseline. To facilitate the control selection, NASA developed a technical specification document that defines security control baselines.[31] Notably, in February 2023, NASA updated the technical specification to add two controls and remove another control from one of its baselines for IT systems.
- **Determine if tailoring the baseline controls is needed.** According to NASA guidance, once a NASA-defined baseline of controls has been selected, system officials are able to tailor the baseline (i.e., remove non-applicable baseline controls or add specific protections outside the control baseline) to meet the needs of the system with a formal written justification.
- **Document the planned control implementations in the system security plan.** NASA guidance requires each control to be documented in the system security plan through the use of implementation statements. These implementation statements should fully address the requirements as laid out in the security control and be understandable by a third-party, with all relevant information provided.
- **Review and approve the system security plan.** At the end of the *select* step, NASA guidance requires authorizing officials to review the system security plan.

NASA fully implemented the key activities in the *select* step for one of the four selected systems. NASA also fully implemented two of the key activities, and partially implemented another key activity, for the remaining three selected systems. Finally, system owners for all four selected systems determined it was not necessary to implement one of the key activities and alter the NASA-defined baseline for their systems.

Officials for each of the systems selected security control baselines for their respective IT systems based on the impact levels assigned to them in the prior step, and none of the systems tailored the selected baselines. In addition, the system security plans for each of the systems that contained planned control implementation information were reviewed and approved in accordance with NASA guidance.

In terms of applying a control baseline, officials from one system included all the appropriate controls for the system's baseline. Due to the criticality of this system, it was designated in RISCS for more stringent control requirements. However, in March 2024, a system official incorrectly removed the more stringent designation in

[30] A security control baseline represents the minimum protection that should be provided to address the impact on an organization's confidentiality, integrity, or availability, as reflected by the system's security category.

[31] NASA Technical Specification, *Control Baselines and Critical Controls for NASA Information Systems Security Configuration Specification,* NASA-SPEC-2661. Controls, v 1.2 (Feb. 21, 2023).

RISCS. Officials for this system acknowledged the mistake and corrected the system’s designation in RISCS in July 2024.[32]

Additionally, NASA officials for the three other selected systems did not fully address this activity because they did not correctly update their corresponding baselines after NASA updated the controls in February 2023. For example, the three systems failed to remove a control that had been in the previous version of the baseline but was removed in the February 2023 version. In addition, one of these three systems did not incorporate two additional controls from the February 2023 update into the relevant baseline for IT systems.

According to NASA officials, there was confusion among the officials from these three selected systems and the NASA information security program team regarding who was responsible for removing the control that had been in the previous version of the relevant baseline. This is because NASA guidance does not define who is responsible for ensuring NASA-defined control baselines are properly applied when baselines are updated. This miscommunication and lack of guidance resulted in the additional control being incorrectly allocated to the three systems. In the case of the system missing the two updated controls from its baseline, during the course of our review, system officials updated the system’s security plans in February 2024 to include the two additional controls from the February 2023 baseline for IT systems that had been missing.

Until NASA updates its guidance to include how system officials should apply agency-defined baseline changes, the agency risks not being able to effectively manage security risks.

NASA Fully Documented Implementation Information for Critical Controls in Security Plans

The purpose of the ***implement*** step is to implement the controls in the security plans for the system and to document the specific details of the control implementation.

Source: GAO analysis of National Institute of Standards and Technology information. | GAO-25-108138

Once the control baseline has been selected as part of the *select* step, NIST and NASA guidance requires that system owners implement and document the implementation information within system security plans.[33] Of the hundreds of controls within each of the systems’ security plans, there is a subset of controls that NASA considers “critical” and are required to be in every plan.

NASA implements and manages its controls using one of the following control types:

- **System-specific controls:** controls that are entirely implemented and managed by the system.
- **Partially inherited controls:** controls where portions of the security controls are implemented and managed by entities other than those responsible for the system.

[32] Specific details of this designation were omitted because the information is considered sensitive.

[33] In the scope of this review, we evaluated whether NASA had documented implementation details for each of the critical controls within the selected baselines for each selected system. According to NASA guidance, critical controls are required to be part of every system’s security plan and cannot be tailored out for any reason. We did not evaluate whether NASA had implemented the controls appropriately. We have ongoing work that is expected to evaluate the implementation of a subset of controls related to the selected systems.

- **Fully inherited controls:** controls in which one system receives protection from security controls that are entirely implemented and managed by entities other than those responsible for the system (i.e., common control providers).

According to NASA guidance, system owners are required to document implementation details within the system's security plan no matter the control type, and to include sufficient implementation information to be used by assessors as part of the *assess* step.

We found that the system owners for all four of the selected systems documented implementation information for each of their critical controls across the three control types.

With the details of the critical control implementation documented, NASA can be better assured that any changes to the controls and their implementation, and the impact of those changes on the security posture, are understood and appropriately authorized.

NASA Partially Implemented Assessment Activities for Selected Systems

The ***assess*** step determines if the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

Source: GAO analysis of National Institute of Standards and Technology and National Aeronautics and Space Administration information guidance. | GAO-25-108138

To ensure that controls are implemented appropriately, NIST and NASA guidance require systems to implement three key assessment activities:

- assessing the implementation of security controls and documenting the results in security assessment reports;[34]
- documenting vulnerability information for unsatisfied controls in security assessment reports; and
- creating remediation plans—POA&Ms and risk-based decisions—based on the findings and recommendations generated from security assessment reports, and executing them in a timely manner.[35]

Two of the four selected systems fully implemented one of the three activities in the *assess* step, and partially implemented the other two activities. The other two selected systems partially implemented all three key activities.

For example, although all four selected systems conducted security control assessments and documented the results in security assessment reports, only two of the systems included assessment results for all of the

[34] For initial assessments (those completed the first time a system is authorized), NASA officials are required to assess all controls. According to NASA guidance, most assessments of previously authorized systems are to be completed on a subset of controls on an annual basis, as part of the continuous monitoring process. The subset of controls in these annual assessments includes a control assessment of all NASA-defined critical controls, and a review of all unsatisfied controls, open POA&Ms, and open risk-based decisions. NASA guidance considers the annual assessments to be part of the *monitor* step. For the purposes of this report, we included the assessment results as part of the *assess* step, because the assessment methodology is the same despite the scope of the assessment being different.

[35] POA&Ms are corrective action plans that document an organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls. Per NASA policy, officials can document a risk-based decision when they plan to accept the risk of not implementing the control instead of developing a plan of action and milestones.

critical controls as required by NASA policy. The two other systems did not completely document assessment results for all critical controls.

Part of the reason for the incomplete security assessment reports is that NASA policy is not clear about how to document assessment results for critical controls that are inherited from common control providers.[36] NASA policy states that all critical controls must be assessed with an extra degree of scrutiny, but also states that inherited controls do not need to be formally reassessed if the control is being inherited correctly. NASA policy does not provide specific guidance on how or whether to document assessment results for controls that are both critical and inherited.

Further, none of the four selected systems documented vulnerability information for unsatisfied controls in complete alignment with NASA guidance. NASA guidance requires system owners to document a description of the vulnerability, a risk discussion, recommendations for remediation, and a residual risk level for unsatisfied critical controls within each system's security assessment report. However, the assessment reports for all four systems lacked remediation recommendations and residual risk levels for unsatisfied critical controls.

Instead, NASA officials documented remedial actions and risk levels in other locations and using other methods. For example, NASA officials used POA&Ms to serve in place of formal recommendations, and documented plans for remediation in RISCS. In the case of inherited critical controls, NASA officials documented recommendations and risk levels in the originating system's security assessment report and did not incorporate that information into the inheriting system's authorization package.

Additionally, none of the four selected systems created remediation plans (e.g., POA&Ms and risk-based decisions) that were in full alignment with NASA policy. This policy requires that POA&Ms feature key information—including risk levels—and that POA&Ms are executed in a timely manner.[37] However, two of the four selected systems did not include risk levels for the majority of POA&Ms, and POA&Ms across all four systems were at least 1 year old during the time of our review. Further, the majority of these systems' POA&Ms were granted an extension beyond their original estimated completion dates.

One explanation NASA officials offered for the missing POA&M risk levels was that risk levels are an optional field within RISCS. In addition, officials noted that NASA policy did not require a risk level at the time the POA&Ms were created. However, NASA guidance from June 2023 and June 2024 states that POA&Ms shall include risk levels. The POA&Ms without risk levels were updated after June 2023; however, these updated POA&Ms failed to include risks levels in accordance with NASA guidance. Regarding POA&M timeliness, NASA officials cited resource constraints; a competing operational project; security priorities; delays in completing dependent tasks; and additional time needed for testing, rollout, and remediation as reasons behind POA&M extensions and delays.

Without the clear and robust establishment and implementation of assessment policies that are aligned with NIST and NASA guidance, NASA runs the risk of having limited visibility into deficiencies related to critical

[36] The majority of the assessment results that were not documented were related to critical controls that were inherited from common control providers.

[37] NASA guidance states that POA&Ms are expected to be completed within 1 year of the POA&M's creation.

security controls. Further, the lack of implementation of assessment policies enables the potential for identified critical security weaknesses to exist unresolved for prolonged periods of time.

NASA Partially Implemented Authorization Activities for the Selected Systems

The purpose of the ***authorize*** step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk associated with the operation of a system or the use of common controls is acceptable.

Source: GAO analysis of National Institute of Standards and Technology information. | GAO-25-108138

To ensure that a system is properly authorized to operate as part of the *authorize* step, NASA guidance requires system officials to implement the following key activities:

- **Create an authorization package.** The authorization package is expected to include relevant system risk information so that the authorizing official can make informed, risk-based decisions. Among other things, this package is to include complete and accurate system security plans, risk assessment reports, security assessment reports, POA&Ms to remediate any identified deficiencies, and documentation of risk acceptances that have been proposed when an issue cannot be remediated.
- **Conduct a risk analysis to support the authorization decision.**
- **Evaluate the risk response actions taken.** Before making an authorization decision, the authorizing official needs to determine whether the team's response to the risk assessment and control assessment has been adequate or needs further work.
- **Make a decision to approve or deny the authorization of the system.**
- **Document the decision.**

Each of the four selected systems have included the necessary documents—including system security plans and security assessment reports—within the packages provided for the most recent authorizations. However, given the deficiencies in documentation that we noted throughout this report, these documents were missing important information that would assist authorizing officials with making fully informed decisions about whether the risks associated with operating the systems were acceptable.

For example, as described throughout this report, the provided authorization packages for the selected systems were missing the required system-level continuous monitoring strategies and key vulnerability information for all unsatisfied critical controls. The authorization packages for three of the selected systems also did not include the proper security control baselines. In addition, none of the four systems executed remedial action within a timely manner for unsatisfied critical controls.

Further, documentation for the selected systems included inconsistent or incomplete information. For example, as previously noted, the impact levels for one system differed across documents, and the documentation inconsistently described whether the system was designated as needing more stringent security requirements. Finally, two of the selected systems did not fully document security assessment results for all critical controls.

As previously described, NASA detailed a variety of reasons for why the authorization packages did not include all the required information, including confusion over guidance or responsibilities. Overall, these shortfalls are partially due to the agency not ensuring that the information developed for the authorization package was appropriate, current, complete, and accurate. This is contrary to OMB guidance for management to identify risks and establish internal controls to provide reasonable assurance that objectives are achieved.[38] In addition, federal internal control standards state that management should use quality information to achieve the entity's objectives and incorporate quality control activities to support the completeness, accuracy, and validity of information.[39] As part of this process, management is expected to periodically evaluate the information to ensure that it is quality information (e.g., appropriate, current, complete, and accurate).

According to NASA officials, the agency's IT Security handbooks describe the responsibilities for ensuring that the information provided to authorizing officials is complete and accurate. The handbooks identify tasks and who is responsible for completing them. For example, the information system owner has overall responsibility to ensure that the authorization package is completed. However, these handbooks do not describe quality control activities for officials to ensure the information was appropriate, current, complete, and accurate. Documenting such activities in its policies would allow NASA to better ensure that it has complete information about the relative risks associated with the operation of the selected systems, and better position NASA's CIO to fully address essential activities needed to manage cybersecurity risks.

NASA Partially Implemented Monitor Activities for Selected Systems

The purpose of the ***monitor*** step is to maintain ongoing situational awareness about the security posture information system and the organization in support of risk management decisions.

Source: GAO analysis of National Institute of Standards and Technology information. | GAO-25-108138

As part of the *monitor* step, NASA guidance requires systems to implement three key activities:

- conducting ongoing assessments of control effectiveness in accordance with an established continuous monitoring strategy;
- identifying, analyzing, and responding to risks on an ongoing basis; and
- updating risk management documents based on the continuous monitoring process.

According to NASA guidance, in most cases these three activities are included as part of an annual assessment of a subset of controls, which is described previously in the *assess* step.[40]

When preparing for continuous monitoring, NASA's guidance requires each information system to have a clearly defined and understood continuous monitoring strategy for the information system. This strategy is to define, among other things, how changes to the system are to be monitored, how risk assessments are to be conducted, and security and privacy posture reporting requirements.

NASA officials from the selected systems provided documentation that summarized the monitoring activities that were conducted during the review process. For example, two of the selected systems provided

[38] Office of Management and Budget, *Management Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123 (Washington, D.C.: July 15, 2016).

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

[40] This subset of controls usually includes (1) all NASA-defined critical controls; (2) all unsatisfied controls, open POA&Ms, and open risk-based decisions; and (3) a selection of other controls. Our evaluation of the adequacy of NASA's ongoing assessment of the selected systems is described as part of the *assess* step.

documentation detailing the various monitoring activities that were conducted as part of a quarterly review process, but not how those fit into a forward-looking continuous monitoring strategy.

However, none of the four selected systems documented system-level continuous monitoring strategies. In particular, none of the systems provided evidence of a documented system-level continuous monitoring strategy that defined how changes to the system were to be monitored, how risk assessments were to be conducted, or security and privacy posture reporting requirements.

NASA officials from two of the selected systems stated that they are not required to import a system-based continuous monitoring strategy into RISCS. In addition, NASA officials stated that they do not have a specific document that lays out a system-level continuous monitoring strategy, and rely on the continuous monitoring tool stated in NASA guidance. However, NASA guidance states that all NASA systems must have a continuous monitoring strategy within their authorization packages.

One reason that the selected systems had not developed continuous monitoring strategies is that NASA's guidance for the monitoring process is still in the process of being updated. Specifically, NASA's continuous monitoring guidance document, which was last updated in June 2024, notes that a future update of the document will include additional guidance on developing and documenting a system's continuous monitoring strategy. However, the version of this guidance documented from January 2022—over 2 years ago—also notes that a future update will include additional guidance in this area.

Without documented strategies that are fully understood by key cyber personnel, organizations face increased risks of data breaches, delayed detection of threats, and slower responses to attacks. Until NASA fully updates its guidance to include clearly defined information on how to develop and document system-level continuous monitoring strategies, and until the selected systems develop continuous monitoring strategies in accordance with the guidance, the agency is at increased risk of inconsistently implementing the continuous monitoring process for its information systems.

Conclusions

Developing, implementing, and maintaining a comprehensive cybersecurity risk management program is critical to protecting NASA's systems and information, detecting suspicious activity, and responding to incidents. Fundamentally, cybersecurity requires understanding the full scope of risks to a system or its data so that those risks can be addressed or accepted. However, key NASA systems did not fully implement selected cybersecurity risk management activities. This could expose the systems to malicious cyber activities such as loss of mission data. The lack of accuracy and completeness of the information used for its cybersecurity risk management process calls into question NASA's oversight of risk management activities. Until the issues with the agency's risk management process are addressed, NASA cannot be sure that the systems helping to propel men and women to the moon—and beyond—are adequately protected.

Recommendations for Executive Action

In our March 2025 CUI report, we made 16 recommendations to NASA. The following recommendations reflect our March 2025 recommendations, but have been modified to remove any information considered to be sensitive:

The NASA Administrator should ensure that NASA's Chief Information Officer prepares and approves an organization-wide cybersecurity risk assessment. (Recommendation 1)

The NASA Administrator should direct NASA's Chief Information Officer to ensure that the documented impact levels for confidentiality, integrity, and availability for all systems match the risk of the system, and that any changes to the provisional impact levels are fully justified in accordance with NASA policy. (Recommendation 2)

The NASA Administrator should direct NASA's Chief Information Officer to update its guidance to include oversight responsibilities for ensuring NASA-defined control baselines are properly applied when baselines are updated. (Recommendation 3)

The NASA Administrator should direct NASA's Chief Information Officer to update its policies to provide more specific guidance about how to document assessment results for all types of critical controls including inherited controls. (Recommendation 4)

The NASA Administrator should direct NASA's Chief Information Officer to ensure that all critical controls for all systems found to be unsatisfied during security control assessments include recommendations and a residual risk level. (Recommendations 5-8)

The NASA Administrator should direct NASA's Chief Information Officer to ensure that POA&Ms related to critical controls for all systems include all key information outlined by its policies and procedures, including risk levels. (Recommendations 9-10)

The NASA Administrator should direct the information system owner for all systems to ensure that estimated completion dates for POA&Ms related to all critical controls for the system are reasonable (e.g. less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. (Recommendations 11-14)

The NASA Administrator should direct NASA's Chief Information Officer to update its policies for the authorize step to include quality control activities to ensure that the information developed for authorization packages is appropriate, current, complete, and accurate. (Recommendation 15)

The NASA Administrator should direct NASA's Chief Information Officer to update NASA's continuous monitoring guidance to provide sufficient information to allow systems to develop clearly defined and understood continuous monitoring strategies, and ensure that selected systems develop continuous monitoring strategies in alignment with the updated guidance. (Recommendation 16)

Agency Comments and Our Evaluation

We provided a draft of the sensitive version of this report to NASA for review and comment. In written comments, NASA concurred with seven recommendations, partially concurred with four recommendations, and did not concur with the remaining five recommendations. The written comments contain information that NASA deemed too sensitive to be released to the public, so we have omitted them from this report. However, we have summarized them below.

In addition, we provided a draft of this report to NASA officials to review and comment on the sensitivity of the information and affirm that the report can be made available to the public without jeopardizing the security of NASA's information systems and networks. The officials confirmed that this report does not include sensitive information and can be released to the public. We also offered the agency the opportunity to provide additional written comments for this version of the report; however, they declined to provide written comments for this public version of the report. The officials also provided technical comments, which we incorporated as appropriate.

For the seven recommendations with which it concurred, NASA described actions it plans to take to address them. In particular:

- NASA concurred with the recommendation to ensure that the impact levels for confidentiality, integrity, and availability for all systems match the risk of the system, and that any changes to the provisional impact levels are fully justified in accordance with NASA policy (recommendation 2). NASA added that the OCIO will work with system owners as well as RISCS developers to make sure these changes are implemented.
- With respect to recommendations aimed at ensuring that NASA documents all key vulnerability information in the security assessment reports for the selected systems (recommendations 5 through 8), NASA's OCIO plans to work with the system owners to ensure that this information is included in security assessment reports where appropriate.
- NASA also concurred with recommendations 9 and 10, and stated that the OCIO will work with the appropriate system owners to ensure that POA&Ms related to critical controls for all systems include all key information outlined by its policies and procedures, including risk levels.

NASA partially concurred with recommendations 11 through 14, which are intended to ensure that estimated completion dates for POA&Ms related to all critical controls for selected systems are reasonable (e.g., less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. NASA did not dispute that POA&M timelines should be reasonable or that POA&Ms should be completed in a timely manner. NASA stated that the responsibility for each system resides with that systems' information system owner rather than the OCIO. It added that the OCIO will work with the system owners to ensure that NASA policies are followed when POA&Ms are created for all critical controls. We have modified recommendations 11 through 14 to reflect that they are now directed to the system owners who are responsible for POA&Ms. We agree that it would be appropriate for the CIO to work with the system owners to ensure that these recommendations are implemented.

NASA did not concur with the remaining five recommendations. Specifically:

- NASA did not concur with recommendation 1, which calls for the CIO to prepare and approve an organization-wide cybersecurity risk assessment. Specifically, NASA stated that instead of an organization-wide cybersecurity risk assessment, the agency uses a near-real time cybersecurity dashboard that aggregates and displays actionable risks that can be identified and remediated at the system level and satisfies the NIST RMF Prepare step.

  However, NASA did not provide evidence showing that the dashboard is sufficiently aggregating risk information for information systems in lieu of a documented organization-wide security risk assessment. Therefore, we believe the recommendation is warranted.

- NASA did not concur with recommendation 3, which calls for the CIO to update NASA's guidance to include oversight responsibilities for ensuring NASA-defined control baselines are properly applied when baselines are updated. Specifically, the agency stated that OCIO oversight is fully documented in policies, procedures, and guidance.

  As previously mentioned in this report, the agency's guidance (including the guidance cited in NASA's response) does not define who is responsible for ensuring NASA-defined control baselines are properly applied to the systems when such baselines are updated. According to officials, there was confusion among the officials from three selected systems and the information security program team regarding who was responsible for making the changes. Due in part to this lack of guidance, three of the selected systems did not apply the February 2023 updates to their associated NASA-defined control baselines. Therefore, we believe the recommendation is warranted.

- NASA did not concur with recommendation 4, which calls for the CIO to provide more specific guidance about documenting assessment results for all types of critical controls including inherited controls. Specifically, NASA stated that existing guidance documents (such as NASA Procedural Requirements 2810.1 and NASA's Assess Handbook) provide sufficient direction on how to document assessment results for all controls.

  The guidance that NASA cited provides information related to documenting assessment results for security controls. However, this guidance does not provide specific information on documenting assessment results for controls that are both critical and inherited. This is one of the reasons why two of our selected systems did not include assessment results for all critical controls as part of the security assessment reports. Thus, we believe this recommendation is still warranted.

- NASA did not concur with recommendation 15, which calls for the CIO to update its policies for the authorize step to include quality control activities to ensure that the information developed for authorization packages is of good quality (i.e., appropriate, current, complete, and accurate). Specifically, NASA stated that the OCIO has policies for the authorize step as well as procedures for oversight related to the information developed for authorization packages.

  As previously mentioned in this report, the agency's guidance (including the guidance cited in NASA's response) does not describe quality control activities for officials to ensure the information was appropriate, current, complete, and accurate. Additionally in October 2024, NASA officials stated there was no specific documentation related to a quality assurance process for the information contained in the RISCS and a system's authorization package. This lack of a quality assurance process is part of the reason for the deficiencies in documentation described throughout this report, including missing, incomplete, and inconsistent information. Having quality information would assist authorizing officials with making fully informed decisions about whether the risks associated with operating the systems were acceptable. Therefore, we believe the recommendation is still warranted.

- NASA did not concur with recommendation 16, which calls for the NASA CIO to update NASA's continuous monitoring guidance. Specifically, the agency stated that its current guidance, particularly their Step 6: Monitor Policy, sufficiently guides systems to develop a system-level continuous monitoring strategy.

  However, none of the four selected systems documented the required system-level continuous monitoring strategies. One reason that the selected systems had not developed continuous monitoring strategies is that the guidance for the monitoring process is still in the process of being updated. NASA's Step 6: Monitor Policy states all systems (including external systems) must have a continuous monitoring strategy and this strategy should be developed by the Information Security Officer with support from the Information

System Security Officer and Information System Security Engineer. However, this guidance document, which was last updated in June 2024, does not contain specific information on how to develop and document a system's continuous monitoring strategy, and states that a future update of the document will include such information. Prior versions of this handbook (approved in January 2022 and June 2023) also contain the same statement that a future update will include additional guidance in this area. Until NASA has fully updated its continuous monitoring guidance, we believe the recommendation is still warranted.

We are sending copies of this report to the appropriate congressional committees, the NASA Administrator, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at WalshK@gao.gov.

GAO staff who made major contributions to this report are listed in appendix II.

//SIGNED//

Kevin C. Walsh
Director, IT and Cybersecurity

List of Requesters

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

The Honorable Mike Haridopolos
Chairman
The Honorable Valerie Foushee
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

The Honorable Frank Lucas
House of Representatives

The Honorable Eric Sorensen
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to assess the extent to which the National Aeronautics and Space Administration (NASA) implemented a cybersecurity risk management program for selected major projects.

In March 2025, we issued a report that assessed the extent that NASA had implemented a cybersecurity risk management program for selected major projects.[1] We designated that report as "controlled unclassified information" (CUI) and did not release it to the public because of the sensitive information it contained. This report publishes the findings discussed in our March 2025 report, but we have removed all references to the sensitive information. Specifically, we deleted the names of the systems that we examined and omitted details from our findings associated with NASA's implementation of key cybersecurity control assessment activities. Additionally, we omitted tables summarizing system-specific findings throughout the report. Although the information provided in this report is more limited, it addresses the same objectives as the sensitive report and uses the same methodology.

To address our objective, we first selected major projects to review. To do so, we first identified NASA projects with a life cycle cost greater than $250 million, by using our 2020–2022 assessments of NASA major projects.[2] We then intentionally selected projects that were managed out of different facilities and covered different phases of development. Based on these criteria, we selected two projects: (1) Gateway Power and Propulsion Element (PPE) from Glenn Research Center and (2) Orion Multi-Purpose Crew Vehicle (Orion) from Johnson Space Center.

We then selected two information systems that are used by each of the selected projects to process, store, and transmit sensitive data. To select these systems, we gathered a list of systems that are used by each project and store, process, and transmit sensitive information. We then selected two systems used by each project based on the types and sensitivity of the data that each system stored, processed, and transmitted.[3] Because of the sensitivity of the information, we have removed the names of the information systems that we examined in this public report.

The results of our review of selected projects and systems are not generalizable to all NASA programs, projects, and systems. However, the selected projects and systems are intended to reflect the experiences and perspectives of projects and systems from across NASA.

To determine the extent to which NASA implemented a cybersecurity risk management program for the selected projects and systems, we reviewed leading cybersecurity practices from the National Institute of Standards and Technology (NIST), including those found in the NIST Risk Management Framework.[4] We also

[1] GAO, *Cybersecurity: NASA Needs to Fully Implement Risk Management*, GAO-25-105882SU (Washington, D.C.: Mar. 12, 2025).

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

[3] The two selected projects use the selected systems, but do not own or manage them.

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

reviewed related NASA cybersecurity risk management guidance documents to determine whether they were consistent with the NIST Risk Management Framework.

As a result of this review, we identified seven cybersecurity risk management steps: (0) *prepare*, (1) *categorize*, (2) *select*, (3) *implement*, (4) *assess*, (5) *authorize*, and (6) *monitor*. For each of these steps, we identified and selected key activities within NASA guidance that we deemed critical to meet the intent of each step. We did not include privacy-related activities within the scope of our review.

For the *prepare* step, which includes activities related to preparing both the organization and the systems to manage cybersecurity risks, we intentionally selected activities to ensure that NASA is ready to carry out essential activities at the organizational level. We reviewed NASA policies, procedures, and guidance for cybersecurity risk management against the key practices for organizational preparation documented in the NIST Risk Management Framework.

For the six other cybersecurity risk management steps, we reviewed agency documentation for each of the selected systems to determine whether NASA had addressed the key activities for each step. To do this, we reviewed documentation that was part of the most recently approved authorization package for each system as of June 2024. This documentation included system security plans, security assessment plans, security assessment reports, plans of action and milestones, documentation of risk-based decisions, and information exported from NASA's data repository for cybersecurity-related system information, known as the Risk Information Security Compliance System.

For the *implement* and *assess* steps, we selected a subset of cybersecurity controls to be part of our review. Specifically, we selected a subset of controls that NASA identified as "critical" and that all systems are required to implement. For the implement step, which includes activities related to implementing controls and documenting the implementation, we evaluated the extent to which NASA documented the implementation of these critical controls. We have ongoing work that is evaluating NASA's implementation of key controls for the selected systems. Because the details of our findings associated with NASA's implementation of the assess step were largely tied to specific systems and security controls deemed to be sensitive, we have omitted some of these details in this public version of the report.

We supplemented and corroborated our analysis of documents and data by interviewing officials in NASA's Office of the Chief Information Officer, and officials for each selected project, about their efforts to implement risk management tasks for their respective systems. We also reviewed and analyzed updated system documentation provided by NASA that had been developed after the authorization packages had been approved.

We made determinations based on the documents and data provided about the extent to which officials for each system implemented the identified key activities for each risk management step.

We rated NASA's actions as "implemented" if NASA provided complete evidence that satisfies the entire selected criterion; "partially implemented" if NASA provided evidence that satisfies some but not all of the selected criterion; and "not implemented" if NASA provided no evidence that satisfies any of the selected criterion.

To assess the reliability of the data we collected on NASA's cybersecurity risk management process, we assessed the data by various means, including reviewing related documentation, examining the system that produced the documentation, and interviewing NASA officials (including NASA's Chief Information Security Officer and relevant officials from each selected project) about the procedures used by the systems to assure accuracy and completeness of the data. Through a combination of methods, we determined that the data used were sufficiently reliable for the purpose of evaluating NASA's efforts to implement a cybersecurity risk management framework for the selected projects.

We also provided a draft of this report to NASA officials to review and comment on the sensitivity of the information and affirm that the report can be made available to the public without jeopardizing the security of NASA's information systems and networks.

The performance audit upon which this report is based was conducted from March 2022 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with NASA from February 2025 to June 2025 to prepare this version of the original CUI report for public release. This public version was also prepared in accordance with these standards.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Kevin C. Walsh, WalshK@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kate Sharkey (Assistant Director), Ahmad Ferguson (Analyst in Charge), Rebecca Eyler, Heather Ko, and Shawn Ward made key contributions to the report. Other staff who made key contributions to the CUI report cited in this report include Alexander Anderegg, Edward Alexander, Tanvir Bhuiyan, Brandon Booth, Kisa Bushyeager, Gilberto Cotto, Saar Dagani, Alan Daigle, Olga Dye, Jennifer Franks, Kathryn Howarth, Michael Lebowitz, Sean Mays, Brandon Mitchell, Jose A. Ramos, W. William Russell, Emmet Ryan, Andrew Stavisky, Joseph Shir, Nathan A. Tranquilli, and Christopher Warweg.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us