NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS
SUITE 8U71, 300 E ST SW
WASHINGTON, D.C. 20546-0001

July 29, 2025

TO: Jeff Seaton
Chief Information Officer

SUBJECT: Final Memorandum, *Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2025* (Report No. IG-25-007; Assignment No. A-25-03-00-MSD)

The Office of Inspector General (OIG) has concluded its required evaluation of NASA's information security program pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2025. This year, Inspectors General were required to assess 25 metrics in 6 security function areas (see Enclosure I for a description of those areas).[1] In addition, we tested a subset of NASA's information systems to determine the maturity of the Agency's information security program.

We assessed NASA's information security policies, procedures, and practices by examining four judgmentally selected Agency information systems and their corresponding security documentation. We also interviewed Agency representatives, including information system owners and personnel responsible for assessing the adequacy of information security controls. In addition, we assessed the Agency's overall cybersecurity posture by (1) leveraging prior work performed by NASA OIG and (2) evaluating the Agency's progress in addressing deficiencies identified in prior FISMA reviews and information security audits. Collectively, the results of these assessments and interviews were the basis for our conclusions.

This year, we rated NASA's information security program at a Level 3 (Consistently Implemented), which means policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking. While this maturity level rating is consistent with the rating NASA received in our past four FISMA reviews, it still falls short of the Office of Management and

[1] The "Govern" security function area was added in fiscal year 2025 to highlight the importance of governance in enterprise risk management. Inspectors General were required to assess this new function and associated supplemental metrics focused on an organization's use of cybersecurity profiles and cybersecurity risk management strategy to guide priorities, constraints, and risk tolerance.

Budget’s Level 4 (Managed and Measurable) rating to be considered effective. See Enclosure II for a description of the maturity level ratings. As required, we submitted the results of this evaluation through the Department of Homeland Security’s CyberScope portal prior to the August 1, 2025, due date.

In addition to our overall assessment of NASA’s information security program, we identified three areas of concern: (1) decentralized cybersecurity risk management and governance, (2) incomplete information system documentation, and (3) inconsistent management of privileged user access.

Decentralized Cybersecurity Risk Management and Governance

NASA has not fully established an integrated and consistent approach to cybersecurity risk management and governance. Although the Agency has developed a cybersecurity risk management strategy, NASA officials could not provide evidence that it updates the strategy annually or reevaluates its risk assumptions and priorities as outlined in National Institute of Standards and Technology guidance.[2] Additionally, key elements—such as cybersecurity profiles, integration of the cybersecurity risk management strategy, and coordinated cyber supply chain risk monitoring—remain underdeveloped or siloed across the Agency.

Cybersecurity profiles help organizations establish a roadmap for reducing cybersecurity risk that is aligned with Agency objectives and can be used to describe the current state or desired target state of specific cybersecurity activities. Without clearly defined and applied cybersecurity profiles, the Agency lacks a standardized method to tailor and communicate cybersecurity objectives across organizational tiers and information systems, thereby limiting its ability to prioritize efforts based on mission and risk context.

The lack of an integrated cybersecurity risk management strategy was evident at the information system level. For example, two of the four sample systems we reviewed did not have a current, approved risk assessment in the Risk Information Security Compliance System—the Agency’s system of record for information security plan documentation—at the time of our initial document request. Additionally, one of those two systems had not conducted a risk assessment since 2016.

Additionally, while NASA conducts cyber supply chain risk assessments at the enterprise (Agency-wide) level that include risk ratings and tailored mitigation recommendations, there is no mechanism to ensure that system owners implement these recommendations and integrate them into system-level risk decisions, nor are risk mitigation efforts centrally tracked. These gaps hinder the Agency’s ability to effectively identify, prioritize, and respond to cybersecurity threats and prevent NASA from managing risk holistically across all organizational tiers.

To address these issues, the Agency has initiated several efforts including development of cybersecurity profiles that align with National Institute of Standards and Technology requirements, updates to its cybersecurity risk management strategy, and improved coordination between enterprise and system-level cyber supply chain risk management activities. However, these initiatives remain in progress and are not yet fully implemented across the Agency.

[2] National Institute of Standards and Technology Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

Incomplete Information System Documentation

We identified documentation for information systems that was missing or incomplete. Specifically, for one of the four sampled systems we reviewed, the control implementation details were not fully documented in its system security plan in the Risk Information Security Compliance System. System officials attributed this to ongoing system development and configuration activities, the prioritization of control implementation over documentation, and limited resources. This issue is consistent with observations from the fiscal year 2023 and fiscal year 2024 FISMA reviews.

Additionally, three of the four systems in our sample did not have comprehensive and up-to-date Business Impact Assessments (BIA) at the time of our initial document request.[3] Specifically, two BIAs did not clearly define acceptable downtimes if a given process was disrupted. The third system was missing a BIA completely. System officials for that system believed they did not need a BIA based on the nature of the system's operations and felt that a risk assessment was sufficient. These gaps hinder the Agency's ability to evaluate the potential impact of system disruptions and implement timely recovery measures.

Inconsistent Management of Privileged User Access

NASA's management of privileged user access remains inconsistent across the Agency.[4] NASA officials indicated that privileged users are not tracked at the enterprise level, which limits the Agency's ability to demonstrate that strong authentication mechanisms are enabled and enforced for all privileged users. Although we found that system officials for one of the four systems in our sample reviewed privileged user accounts, the processes for provisioning, managing, and reviewing these accounts periodically were not consistently implemented at all organizational levels. Similarly, because there is no centralized tracking, NASA officials could not demonstrate that all privileged users are required to use strong authentication for physical entry and exit at defined points. We continue to monitor the Agency's progress on implementing a recommendation related to this issue from a prior evaluation (see Enclosure III for details on this and other open recommendations from previous FISMA reviews).

Status of Prior FISMA Recommendations

NASA has made progress in implementing recommendations from prior FISMA reviews. During fiscal years 2024 and 2025, NASA implemented corrective actions for 22 of 27 open recommendations and continues to work to implement the remaining recommendations to further improve its information security program. While we are not making any formal recommendations this year, we did communicate these new and recurring issues to NASA management. We will continue to monitor these issues and the status of prior open recommendations during the fiscal year 2026 FISMA evaluation.

[3] A Business Impact Assessment is an analysis of an information system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

[4] A privileged user is a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

We discussed this memorandum with Agency officials and incorporated technical changes where appropriate. If you have questions or wish to comment on the quality or usefulness of this memorandum, please contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Brian Mullins
Acting Assistant Inspector General for Audits

Enclosures—3

Enclosure I: Cybersecurity Framework Function Areas

For the fiscal year 2025 evaluation of agency information security programs under FISMA, Inspectors General were required to assess six security function areas. Table 1 describes those six areas along with the related National Institute of Standards and Technology cybersecurity framework categories.

Table 1: Function Areas and Related Categories

Function Area	Description	Related Cybersecurity Framework 2.0 Categories
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	• Organizational Context • Risk Management Strategy • Roles, Responsibilities, and Authorities • Policy • Oversight • Cybersecurity Supply Chain Risk Management
Identify	The organization's current cybersecurity risks are understood.	• Asset Management • Risk Assessment • Improvement
Protect	Safeguards to manage the organization's cybersecurity risks are used.	• Identity Management, Authentication, and Access Control • Awareness and Training • Data Security • Platform Security • Technology Infrastructure Resilience
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	• Continuous Monitoring • Adverse Event Analysis
Respond	Actions regarding a detected cybersecurity incident are taken.	• Incident Management • Incident Analysis • Incident Response Reporting and Communication • Incident Mitigation
Recover	Assets and operations affected by a cybersecurity incident are restored.	• Incident Recovery Plan Execution • Incident Recovery Communication

Source: National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (February 26, 2024).

Enclosure II: Inspector General Evaluation Maturity Levels

Inspectors General can assign one of five maturity level ratings to their agency's information security program. Table 2 outlines those maturity level ratings and provides a description of each. As noted, we rated NASA's information security program at a Level 3 (Consistently Implemented) for fiscal year 2025. To be considered effective, the information security program should be rated at a Level 4 (Managed and Measurable).

Table 2: Maturity Levels and Descriptions

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: Cybersecurity and Infrastructure Security Agency, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (April 3, 2025).

Enclosure III: Open FISMA Recommendations from Prior Fiscal Years

We close recommendations from prior reviews if corrective actions were completed and verified. However, if recommended or additional corrective actions are necessary, prior recommendations will remain open until evidence is provided that adequately satisfies the intent of the recommendation. Table 3 lists the recommendations we made in prior FISMA reviews that remain open as of July 2025. All of the recommendations noted below are from fiscal year 2023.

Table 3: Open FISMA Recommendations from Fiscal Year 2023

Recommendation	Status of Recommendation
Recommendation 8: Revise its policies and procedures to document and implement a lessons learned process based on risk events within the Information Security Continuous Monitoring (ISCM) and Risk Management areas. System security personnel should be instructed to record, analyze, and revise control activities to improve NASA's security posture.	**Open** Revised Completion Date: 9/30/2025
Recommendation 11: Continue to implement the necessary entity-wide oversight to improve enforcement mechanisms and controls to ensure all standard baselines and vulnerabilities are monitored and remediated in accordance with Federal and Agency requirements.	**Open** Revised Completion Date: 7/31/2025
Recommendation 15: Ensure that the security controls in control families Program Management (PM), Personally Identifiable Information Processing and Transparency (PT), and Supply Chain Risk Management (SR) are updated and defined within the Agency's ISCM strategy.	**Open** Revised Completion Date: 9/30/2025
Recommendation 16: Document the NASA Manual Inventory process in NASA's ISCM Strategy to ensure its hardware inventory monitoring process is accurate, complete, and fully aligns with NASA's other continuous monitoring guidance and integrates processes, associated outputs, and incorporates results to provide situational awareness.	**Open** Revised Completion Date: 9/30/2025
Recommendation 20: Continue its efforts to prioritize projects that address the complexities required across Event Logging (EL) tiers to meet the intermediate (EL2) maturity level in accordance with the Office of Management and Budget’s M-21-31.	**Open** Revised Completion Date: 11/30/2028

Source: NASA OIG.