NASA OFFICE OF INSPECTOR GENERAL

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

September 16, 2026

TO: Sean Gallagher
Chief Information Officer

SUBJECT: Final Memorandum, *Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2026*
(Report No. IG-26-013; Assignment No. A-26-04-00-MSD)

The Office of Inspector General 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 2026. This year, Inspectors General were required to assess 25 metrics in 6 security function areas. See Enclosure I for a description of those areas. 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 the NASA Office of Inspector General 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. This maturity level rating is consistent with the ratings NASA has received in our prior FISMA reviews over the last 5 years, yet still fell short of the Office of Management and Budget's Level 4 (Managed and Measurable) rating to be considered effective. See Enclosure II for a description of the maturity levels. As required, we submitted the results of this evaluation through the Department of Homeland Security CyberScope portal prior to the July 31, 2026, due date.

In addition to our overall assessment, we identified two recurring areas of concern: (1) the absence of formal cybersecurity profiles and (2) outdated information system documentation.

Cybersecurity Profiles

We found the Agency has not yet established policies or procedures for developing and maintaining formal cybersecurity profiles, and as a result, has not implemented current or target profiles. A cybersecurity profile is a documented representation of an organization's current or desired cybersecurity posture. 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. While certain cybersecurity objectives were informally referenced in various policy documents, NASA lacks an enterprise-wide process to assess, prioritize, or communicate those objectives. 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. To its credit, NASA has an initiative to establish cybersecurity profiles and related governance processes, but the effort is still in progress and is not yet fully implemented.

Information System Documentation

We noted outdated information system security documentation was maintained within the Risk Information Security Compliance System, NASA's system of record for information system security plans. Of the four information systems in our sample, two had Authorization to Operate reviews that were past due.[1] Additionally, two of the four systems had past-due Plans of Action and Milestones and/or Risk Based Decisions.[2] Further, one system's contingency plan was outdated, unsigned, and did not represent the system's current operating environment. Incomplete information system documentation is a recurring issue that we have identified in prior year reviews. These gaps hinder the Agency's ability to evaluate the potential impact of system disruptions and implement timely recovery measures.

[1] Authorization to Operate is the official management decision to authorize operation of an information system and accept the risk to agency operations, including mission, functions, image, or reputation, agency assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

[2] Plans of Action and Milestones is a document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones. Risk Based Decisions is the documented process used to formally accept risk for known weaknesses or vulnerabilities in an information system, based on an authorizing official's analysis to make a credible determination regarding the continued operation or use of the system or the provision of common controls.

While we are not making any formal recommendations this year, we did communicate these recurring issues to NASA management. We will continue to monitor these issues during the fiscal year 2027 FISMA evaluation. 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
Deputy Assistant Inspector General for Audits

Enclosures—2

Enclosure I: Cybersecurity Framework Function Areas

For the fiscal year 2026 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 2026. 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).