NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS
SUITE 8U71, 300 E ST SW
WASHINGTON, DC 20546-0001

September 12, 2024

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 2024*
(IG-24-019; A-24-01-00-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 (FY) 2024. For FY 2024, Inspectors General were required to assess 65 metrics in 5 security function areas. In addition, we tested a subset of information systems to determine the maturity of the Agency's information security program. (See Enclosure I for a description of the 5 security function areas.)

We assessed NASA's information security policies, procedures, and practices by examining four judgmentally selected Agency information systems along with 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 work performed by NASA OIG and other oversight organizations, including the Government Accountability Office 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.

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 rating is consistent with ratings in the prior 3 years, yet still fell short of the Office of Management and Budget's rating that agency cybersecurity programs are required to meet to be considered effective (Level 4: Managed and Measurable). (See Enclosure II for a description of the maturity levels.) As required, we submitted the results of this review through the Department of Homeland Security CyberScope portal on the due date of July 31, 2024.

In addition to our overall assessment, we identified two areas of concern: (1) information system documentation maintained outside of the Agency's system of record and (2) enterprise-level risk and privacy activities not conducted. During our testing of the four sample systems, we noted that for one system, the information system security plan documentation was not maintained in Risk Information Security Compliance System (RISCS)—NASA's system of record for information system security plans. Instead, system owners opted to use a separate location to store and manage security system plan documentation. System owners cited a need for more controlled access to security plan documentation, as well as the level of sensitive proprietary data, making it easier to manage security documentation outside of RISCS. We identified similar issues with the usage of RISCS in our last FISMA evaluation.[1]

We also noted that NASA has not performed enterprise-level risk activities, such as Agency-level cybersecurity and privacy risk assessments. A core FISMA metric outlines that organizations should use the results of system level risk assessments and other inputs to develop and maintain cybersecurity risk registers and enterprise risk management programs to monitor the effectiveness of risk responses and ensure that risk tolerances are maintained at an appropriate level. Agency officials explained that due to NASA's unique mission, enterprise-wide assessments are not currently conducted. The prior FISMA evaluation also identified a lack of an enterprise-wide risk register. We communicated these recurring issues to NASA management during our review and plan to continue to monitor them during the FY 2025 FISMA evaluation.

We appreciate the courtesies and cooperation provided during this review. If you have any questions or would like to discuss these results further, please contact Tekla Colón, Mission Support Director, Office of Audits, at 202-358-2583 or tekla.m.szelong@nasa.gov, or Scott Riggenbach, Assistant Director, at 321-867-5331 or scott.a.riggenbach@nasa.gov.

Kimberly Benoit

Digitally signed by Kimberly Benoit
Date: 2024.09.11 08:40:14 -04'00'

Kimberly F. Benoit
Assistant Inspector General for Audits

Enclosures—2

[1] *NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023* (IG-23-017, August 17, 2023).

Enclosure I: Cybersecurity Framework Function Areas

Table 1: Function Areas

Function Area	Description
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

Source: National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0.

Enclosure II: Inspector General Evaluation Maturity Levels

Table 2: Maturity Levels and Descriptions

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

Source: Cybersecurity and Infrastructure Security Agency— *FY 2023 – 2024 IG FISMA Reporting Metrics*.