NASA OFFICE OF INSPECTOR GENERAL

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

November 9, 2021

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 2021* (A-21-012-00; ML-22-001)

The Office of Inspector General (OIG) has concluded its review of NASA's information security program pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2021. For FY 2021, Inspectors General were required to assess 66 metrics in 5 security function areas and test a subset of information systems to determine the maturity of their agency's information security program. (See Enclosure I for a description of the five security function areas.) To fulfill this requirement, 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 the security of the four systems reviewed. In addition, we assessed the Agency's overall cybersecurity posture by (1) leveraging work performed by NASA 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 assisted us in reaching our conclusions.

In summation, we rated NASA's cybersecurity program at a Level 3 (Consistently Implemented), which marks an increased assessed maturity level over the past four years. However, this year's maturity level still falls short of the Level 4 rating (Managed and Measurable) agency cybersecurity programs are required to meet by the Office of Management and Budget in order to be considered effective. (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 web portal on October 26, 2021. Moving forward, we encourage the Agency to continue to mature its information security program and strengthen its cybersecurity efforts.

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 Mark Jenson, Financial Management Director, Office of Audits, at 202-358-0629 or mark.jenson@nasa.gov, or Joseph Shook, Project Manager, at 216-433-9714 or joseph.a.shook@nasa.gov.

Kimberly Benoit

Digitally signed by Kimberly Benoit
Date: 2021.11.09 06:46:32 -05'00'

Kimberly F. Benoit
Assistant Inspector General for Audits

cc: Mike Witt
Associate Chief Information Officer for Cybersecurity and Privacy

Cody Scott
Chief Cyber Risk Officer

Joseph Mahaley
Assistant Administrator for Protective Services

Enclosures – 2

Enclosure I: Cybersecurity Framework Function Areas

Table 1: Function Area Descriptions

Function Area	Description
Identify[a]	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.

[a] The FY 2021 Inspector General FISMA Reporting Metrics included a new domain on Supply Chain Risk Management (SCRM) within the Identify function. This new domain focused on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. The metric ratings for SCRM were not considered when determining the maturity level of the "Identify" function by design of the FY 2021 rating instructions.

Source: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018).

Enclosure II: Inspector General Evaluation Maturity Levels

Table 2: Maturity Level Descriptions

Maturity Level	Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized, and 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, consistently implemented, and regularly updated based on a changing threat and technology landscape and business or mission needs.

Source: FY 2021 Inspector General FISMA Reporting Metrics.