NASA OFFICE OF INSPECTOR GENERAL

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

March 6, 2019

TO: Renee Wynn
Chief Information Officer

SUBJECT: *Review of NASA's Information Security Program under the Federal Information Security Modernization for Fiscal Year 2018 Evaluation* (A-18-007-00; ML-19-002)

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) 2018. For FY 2018, Inspectors General were required to assess 61 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 5 security function areas.) We assessed NASA's information security policies, procedures, and practices by examining 7 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 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.[1] Collectively, the results of these assessments and interviews assisted us in reaching our conclusions.

In sum, we rated NASA's cybersecurity program at a Level 2 (Defined) for the second year in a row, which falls short of the Level 4 (Managed and Measurable) rating 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 in late October 2018.

[1] NASA OIG, *Audit of NASA's Information Technology Supply Chain Risk Management Efforts* (IG-18-019, May 24, 2018); *Audit of NASA's Security Operations Center* (IG-18-020, May 23, 2018); *Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation* (IG-18-003, November 6, 2017); *Industrial Control System Security Within NASA's Critical and Supporting Infrastructure* (IG-17-011, February 8, 2017); and *Security of NASA's Cloud Computing Services* (IG-17-010, February 7, 2017).

In addition to our overall assessment, we identified two areas of concern: (1) system security plans contained missing, incomplete, and inaccurate data and (2) information system control assessments were not conducted in a timely manner. We consider the issue of missing, incomplete, and inaccurate information security plan data to be an indicator of a continuing control deficiency that we have identified in recent NASA OIG reviews.[2] Likewise, the untimely performance of information security control assessments could indicate control deficiencies and possibly significant threats to NASA operations, which could impair the Agency's ability to protect the confidentiality, integrity, and availability of its data, systems, and networks. We communicated these issues to NASA management during the course of our review and plan to more fully explore them during our FY 2019 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 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.

Jim Morrison
Assistant Inspector General for Audits

cc: Daniel J. Tenney
Associate Administrator for Mission Support Directorate

Joseph Mahaley
Assistant Administrator for Protective Services

Enclosures – 2

[2] IG-18-019 and IG-17-010.

Enclosure I: Cybersecurity Framework Function Areas

Table 1: Function Area Descriptions

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, *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 with activities 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/mission needs.

Source: FY 2018 Inspector General FISMA reporting metrics.