NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

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

August 17, 2023

TO: Jeff Seaton
Chief Information Officer

SUBJECT: Final Report, *NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023* (Report No. IG-23-017; Assignment No. A-23-03-00-FMD)

The Federal Information Security Modernization Act of 2014 (FISMA) requires the NASA Office of Inspector General (OIG), or an independent external auditor, to conduct an annual evaluation of NASA's information security program. The OIG selected the independent public accounting firm RMA Associates, LLC (RMA) to evaluate NASA's information security program in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* and against the fiscal year 2023 Inspector General FISMA Reporting Metrics.

This evaluation resulted in rating 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 fell short of the Office of Management and Budget's rating that indicates an agency's cybersecurity program is effective.

In our oversight of the contract, we reviewed RMA's reports and related documentation and inquired of its representatives. RMA is responsible for the enclosed report and the conclusions expressed therein.

We appreciate the courtesies and cooperation extended to our team during the evaluation. Please contact Brian Mullins, Acting Assistant Inspector General for Audits, at 202-358-0725 or brian.mullins@nasa.gov, if you have any questions about the enclosed report.

Pursuant to PL 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to HQ-Section5274Submissions@nasa.gov within 30 days of the report issuance date, and we request that comments not exceed 2 pages. The comments will be appended by link to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

PAUL
MARTIN

Digitally signed by
PAUL MARTIN
Date: 2023.08.16
17:05:49 -04'00'

Paul K. Martin
Inspector General

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

Enclosure–1

National Aeronautics and Space Administration
Federal Information Security Modernization Act of 2014

Evaluation Report for Fiscal Year 2023

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

August 17, 2023

Mr. Paul K. Martin
Inspector General
300 E St SW
Washington, DC 20546

Mr. Jeffrey Seaton
Chief Information Officer
300 E St SW
Washington, DC 20546

Re: National Aeronautics and Space Administration's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023

RMA Associates, LLC is pleased to submit the National Aeronautics and Space Administration (NASA) Federal Information Security Modernization Act of 2014 (FISMA) Evaluation Report for fiscal year (FY) 2023. The objective of this evaluation was to evaluate the effectiveness of NASA's information security program and practices for the period October 1, 2022, through May 31, 2023. We conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, issued in December 2020.

For FY 2023, the Office of Management and Budget (OMB) identified 20 core and 20 supplemental Inspector General metrics to be evaluated. These metrics are outlined in OMB's *FY 2023 – 2024 Inspector General (IG) FISMA Reporting Metrics* Version 1.1, dated February 10, 2023. The Inspector General is required to assess the maturity levels of these metrics.

As part of our evaluation, we conducted an assessment of the FY 2023 core and supplemental metrics on behalf of NASA's Office of Inspector General (OIG). The results of this assessment are presented in Appendix A – NASA OIG FY 2023 IG CyberScope Submission.

In summary, we found NASA's information security program and practices were not effective for the period October 1, 2022, through May 31, 2023.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

Table of Contents

Introduction

This report presents the results of RMA Associates, LLC's (RMA) independent evaluation of the National Aeronautics and Space Administration (NASA) information security program and practices for fiscal year (FY) 2023. The Federal Information Security Modernization Act of 2014 (FISMA)[1] requires Federal agencies to have an annual independent evaluation of their information security program and practices to determine the effectiveness of such programs and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB delegated its responsibility to the U.S. Department of Homeland Security (DHS) for the collection of annual FISMA responses.

NASA's Office of Inspector General (OIG) engaged RMA to conduct the annual evaluation of NASA's information security program and practices in support of the FISMA evaluation requirement. The objective of this evaluation was to evaluate the effectiveness of NASA's information security program and practices for the period October 1, 2022, through May 31, 2023.

As part of our evaluation, we responded to the FY 2023 20 core and 20 supplemental metrics specified in OMB's *FY 2023 – 2024 Inspector General (IG) FISMA Reporting Metrics*, Version 1.1, dated February 10, 2023.[2] We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards. Our responses to the FY 2023 20 core and 20 supplemental metrics are provided in Appendix A – NASA OIG FY 2023 IG CyberScope Submission. These core and supplemental metrics provide reporting requirements across the functional areas to be addressed in independent assessments of agencies' information security programs.

Summary Evaluation Results

We concluded that consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, NASA's information security program and practices were established and maintained for the five Cybersecurity Functions[3] and nine FISMA Metric Domains.[4] The overall maturity level of NASA's information security program was determined as Consistently Implemented, as described in this report. Within the context of the FISMA maturity model, Managed and Measurable represents an effective level of security. As such, we found

[1] FISMA, Pub. L. No. 113-283, 128 Stat. 3073 (December 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521.

[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the IG FISMA Reporting Metrics in consultation with the federal Chief Information Officers Council.

[3] The five Cybersecurity Functions as defined in the NIST Cybersecurity Framework are: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover.

[4] As described in the IG FISMA Reporting Metrics, the nine FISMA Metric Domains, which are aligned with the five Cybersecurity Functions, are: (1) risk management, (2) supply chain risk management (3) configuration management, (4) identity and access management, (5) data protection and privacy, (6) security training, (7) information security continuous monitoring, (8) incident response, and (9) contingency planning.

NASA's information security program and practices were not effective for the period October 1, 2022, through May 31, 2023.

We provided NASA with a draft of this report for comment. NASA concurred on all 27 recommendations. See *Management's Response* in Appendix C for NASA's response in its entirety.

Background

National Aeronautics and Space Administration

NASA is America's civil space program and the global leader in space exploration. The Agency has a diverse workforce of just under 18,000 civil servants and works with many more U.S. contractors, academia, and international and commercial partners to explore, discover, and expand knowledge for the benefit of humanity.

At its 20 centers and facilities across the country – and the only National Laboratory in space – NASA studies Earth, including its climate, our Sun, solar system, and beyond. NASA also conducts research, testing, and development to advance aeronautics, including electric propulsion and supersonic flight. Additionally, NASA develops and funds space technologies that will enable future exploration and benefit life on Earth.

NASA also leads a Moon to Mars exploration approach, which includes working with U.S. industry, international partners, and academia to develop new technology, and send science research and soon humans to explore the Moon on Artemis missions that will help prepare for human exploration of the Red Planet. In addition to those major missions, the Agency shares what it learns so that its information can make life better for people worldwide. For example, companies use NASA discoveries and technologies to create new products for the public. To ensure future success for the Agency and the nation, NASA also supports education efforts in science, technology, engineering, and mathematics with an emphasis on increasing diversity in our future workforce.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes Title III, entitled the Federal Information Security Management Act of 2002 (FISMA 2002). Title III required each Federal Agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the Agency, including those provided or managed by another agency, contractor, or other sources.

On December 18, 2014, the President signed FISMA 2014, which amended FISMA 2002 and provided several modifications that modernized Federal security practices to address evolving security concerns. These changes resulted in less overall reporting, strengthened the use of continuous monitoring systems, increased focus on the agencies for compliance, and produced reporting more focused on the issues caused by security incidents.

FISMA requires federal agencies to have an annual, independent assessment performed of their information security programs and practices to determine the effectiveness of such programs and practices and report the assessment results to OMB. In addition to the annual review and reporting requirements, FISMA included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, *Managing Federal Information as a Strategic Resource*, requires executive agencies within the federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibilities;
- Periodically review the security controls in their systems; and
- Authorize system processing prior to operations and periodically after.

These management responsibilities presume responsible agency officials understand the risks, and other factors, which could adversely affect their missions. Moreover, these officials must understand the current status of their security programs, and the security controls planned or in place to protect their information and systems to make informed judgments and investments which appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

FISMA provided OMB oversight authority of agency security policies and practices and provided authority for implementing agency policies and practices for information systems to DHS.[5]

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives requiring agencies to implement OMB's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.[6] It authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[7]

Additionally, FISMA directed federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the U.S. Government

[5] FISMA, Pub. L. No. 113-283, 128 Stat. 3073 (December 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[6] Ibid.
[7] Ibid.

Accountability Office (GAO). Reports are required to include: (1) threats and threat factors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents (3) the status of compliance of the systems at the time of the incidents; (4) detection, response, and remediation actions; (5) the total number of incidents; and (6) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[8]

Key Changes to the FY 2023 IG FISMA Metrics

One of the annual FISMA evaluation goals was to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the Administration's priorities and best practices. OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, on December 2, 2022, that provides guidance on how OMB and CIGIE are transitioning the IG metrics process to a multi-year cycle and other guidance, such as directing federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts. Using a multi-year cycle, a core group of metrics must be evaluated annually and the remainder of the standards and controls will be evaluated in metrics on a 2-year cycle. The multi-year cycle approach was agreed to by CIGIE, OMB, the federal Chief Information Security Officer (CISO) Council, and DHS's Cybersecurity & Infrastructure Security Agency (CISA).

As a representation of this guidance, on February 10, 2023, the final IG FISMA Metrics for FY 2023 were released,[9] which included the 20 core metrics plus an additional 20 supplemental metrics to be assessed in the FY 2023 review cycle. The remaining supplemental metrics will be tested during the review cycle for FY 2024.

Additionally, OMB Memorandum M-23-03 solidifies the adjustment of the timeline for the IG evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle to facilitate the timely funding for the remediation of problems identified. Historically, IG evaluation of agency effectiveness finished in October until FY 2022, when the deadline shifted to July 31 of each year. However, OMB granted NASA OIG an extension to submit the FY 2022 IG CyberScope results by September 30, 2022. For FY 2023, the IG evaluation has a deadline of July 31, 2023, for FISMA reporting to OMB and DHS.

Finally, in previous years, IGs were directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied at the function and overall information security program level. However, OMB and CIGIE determined this was not the best approach. The approach for FY 2023 will focus on a calculated average approach (instead of mode), wherein the average of the metrics in a particular domain will be used by IGs to determine

[8] Ibid.
[9] DHS, *FY 2023 – 2024 IG FISMA Reporting Metrics* (February 10, 2023).

the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

IG FISMA Reporting Metrics

For FY 2023, we assessed the group of core metrics, which represents a combination of administration priorities and other highly valuable controls selected by OMB that must be evaluated annually. Additionally, we tested the 20 supplemental metrics identified for the FY 2023 review cycle.

The IG metrics represent a continuation of work begun in FY 2016 when the IG metrics[10] were aligned with the five (5) function areas in NIST's Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.[11] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. IGs assess each of these function levels against the listed criteria when assigning the Agency's performance metric rating.

We evaluated the effectiveness of information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. DHS's IG FISMA Reporting Metrics classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized (**Table 1**). Within the context of the maturity model, per OMB Level 4, Managed and Measurable represents an effective level of security.

Table 1: IG Evaluation Maturity Levels

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.

Evaluation Results

In FY 2023, a calculated average scoring model was used, where core and supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points

[10] DHS, *FY 2016 IG FISMA Reporting Metrics*, Version 1.1.3 (September 2016).
[11] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 2018).

for the assessed program and function effectiveness. For example, if the calculated core metric maturity of two of the function areas is Level 3: Consistently Implemented (i.e., 3.0) and the computed core metric maturity of the remaining three function areas is Level 4: Managed and Measurable (i.e., 4.0), the information security program rating would average to be a 3.60 (i.e., (3+3+4+4+4)/5).

RMA focused on the results of the core metrics to determine maturity levels and used the calculated averages of the supplemental metrics as a data point to support our risk-based determination of overall program and function level effectiveness. The overall maturity level of the information security program was assessed as Consistently Implemented and, as such, was not effective for the period October 1, 2022, through May 31, 2023. Although the DHS calculated average of the maturity level was 2.67, the Defined level, we concluded NASA's maturity level was Consistently Implemented. NASA's control processes were operational and generated information that supported control monitoring and decision making and, thus, exceeded a maturity level of Defined. The Defined level did not accurately depict NASA's control environment. However, we identified certain weaknesses in the control process that hindered their effectiveness. In addition, more controls need to be implemented in addition to those tested for NASA to reach Managed and Measurable, which is OMB's benchmark for an effective information security program. As a result, NASA's overall maturity level was Consistently Implemented and not effective.

NASA's FY 2023 calculated maturity averages and assessed maturity level by function are presented in **Table 2**.

Table 2: NASA's FY 2023 Calculated Maturity Averages and Assessed Levels

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity Average[12]	FY 2023 Assessed Maturity
Identify	2.17	2.6	2.38	Defined
Protect	3.25	3.7	3.48	Consistently Implemented
Detect	2.0	2.0	2.0	Defined
Respond	3.0	4.0	3.5	Consistently Implemented
Recover	2.0	2.0	2.0	Defined
Overall Maturity	**2.48**	**2.86**	**2.67**	**Consistently Implemented**

NASA's maturity and effectiveness levels have remained the same from the prior year and are presented in **Table 3**.

Table 3: FY 2022 – FY 2023 Maturity Level Comparison

Function	FY 2022 Assessed Maturity	FY 2023 Assessed Maturity
Identify	Defined	Defined

[12] In FY 2023 the DHS calculated maturity average was computed by averaging the core and supplemental metrics and the calculated averages were not rounded to determine the maturity level. In determining maturity levels and the overall effectiveness of NASA's information security program, RMA focused on the results of the core metric and made a risk-based assessment of overall program and function level effectiveness.

Function	FY 2022 Assessed Maturity	FY 2023 Assessed Maturity
Protect	Consistently Implemented	Consistently Implemented
Detect	Defined	Defined
Respond	Consistently Implemented	Consistently Implemented
Recover	Consistently Implemented	Defined
Overall Maturity	**Consistently Implemented**	**Consistently Implemented**
Overall Effectiveness	**Not Effective**	**Not Effective**

The Office of the Chief Information Officer (OCIO) is required to monitor and evaluate the performance of information system programs and practices based on performance measurements. The following paragraphs provide more details on each functional area's assessed maturity level and provide the OCIO with recommendations to remediate deficiencies.

IDENTIFY FUNCTION

The Identify Function relates to developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effectively using the Cybersecurity Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.[13] The domains included under this function are Risk Management and Supply Chain Risk Management. We determined the Identity Function's maturity level was Defined and not effective.

Risk Management: We determined NASA's overall maturity level for the Risk Management program was Defined. NASA used its Risk Information Security Compliance System (RISCS) as the system of record for information systems. RISCS provides an automated centralized, enterprise-wide portfolio of NASA's information security systems including hardware and software whether on-premises, cloud-based, or third-party systems, and system interconnections. Multiple sources and tools supplement RISCS to manage the compliance of NASA's information.

We noted that certain information in RISCS was not current. Specifically, RMA determined:

Two systems selected for testing during the FY 2022 FISMA evaluation were listed as operational in RISCS but were not in use. In FY 2023, we tested four additional systems and found no system inventory discrepancies. However, corrective action for the two systems identified had not been completed. (NFR FY23-FISMA-10)

One of the systems selected for testing could not provide evidence to demonstrate an up-to-date inventory of all licenses used within its system boundaries. A similar issue was noted in the prior year when another system’s inventory did not include all of its software assets and licenses. NASA Procedural Requirements 2810.1F, *Security of Information and Information Systems* and NIST

[13] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, require software inventory and license tracking. Although NASA began establishing a centralized information technology governance structure that provides oversight to ensure the Information System Owners (ISOs) maintain accurate information in RISCS, this process was not completed due to the prioritization of other projects. Without accurate and up-to-date system inventory and licensing information in RISCS, the Agency may make decisions on erroneous or incomplete software assets and license data, which could impact its ability to provide NASA-wide oversight for its software assets and licenses. (NFR FY23-FISMA-03)

In addition, NASA did not have policies, procedures, and processes for risk framing, risk response, and risk monitoring to manage cybersecurity risks. Although the Agency had begun developing such, development was delayed to prioritize other projects. By not defining policies, procedures, and processes around risk framing, risk response, and risk monitoring, NASA increases its inability to identify trends and implement strategies to mitigate and effectively monitor its risks. (NFR FY23-FISMA-02)

Further, NASA did not complete the development of an enterprise-wide risk register or a risk profile to record, track, and communicate enterprise-wide cybersecurity risk management data to support enterprise-level decision-making and activities across the Agency. OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, requires agencies to develop and maintain risk registers and profiles. Although NASA had begun maturing its Enterprise Cyber Risk Management function, due to the reorganization across the enterprise and the prioritization of other initiatives, the Agency did not complete its development of risk registers or risk profiles. Without risk registers or risk profiles, NASA may not be able to anticipate and protect from threats to confidentiality, integrity, and availability of information and systems in a timely manner. (NFR FY23-FISMA-01)

In response to our recommendations from the FY 2022 FISMA evaluation, NASA developed a corrective action plan with an estimated completion date of November 17, 2023. As a result, the recommendations were not implemented during our evaluation period. The recommendations have been reissued to address current and prior year findings.

Recommendations:

RMA recommends the OCIO:

1. Implement necessary oversight to monitor RISCS for accuracy and completeness, so RISCS provides sufficient support for decision-making and determining compliance with federal requirements. (NFR FY23-FISMA-10)
2. Ensure the information system owner of the systems selected for testing perform a system inventory of software assets and licenses used within the system boundaries and updates RISCS as necessary. (NFR FY23-FISMA-03)
3. Implement necessary oversight to monitor RISCS for accuracy and completeness of software and license information. (NFR FY23-FISMA-03)
4. Continue its efforts in developing policies, procedures, and processes for risk framing, risk response, and risk monitoring. (NFR FY23-FISMA-02)

5. Continue its efforts to develop and implement the necessary entity-wide oversight policy and procedures to monitor risk through a risk register and a risk profile that provide enterprise-wide metrics to inform top management of its Information Technology (IT) risks. (NFR FY23-FISMA-01)

NASA manages its Plans of Actions and Milestones (POA&Ms) to address security weaknesses and prioritize remediation efforts. In our FY 2022 FISMA evaluation, we found that POA&Ms and Risk Based Decisions (RBDs) were not updated and approved in a timely manner. In our FY 2023 FISMA evaluation, we continued to find POA&Ms were not completed within the milestone dates. Specifically, two of the four selected systems had POA&Ms significantly past their completion due dates. NASA's Information Technology Security Handbook (ITS-HBK), *STEP 6: Monitor Policy* (ITS-HBK-AASTEP6. V.1.0.0), requires all POA&Ms be reviewed and/or updated at least annually in RISCS by the ISO and approved by the Approving Official, as part of its continuous monitoring. According to NASA management, the past due POA&Ms resulted from the reorganization across the enterprise and conversion of policies and procedures to NIST SP-800-53 Revision 5. NASA management also stated that updating and approving POA&Ms involves multiple layers of reviews, which may cause delays in the approval process. Past due POA&Ms and unapproved RBDs may negatively impact the overall risk exposure at NASA. As a result, the Agency may not accurately measure risks related to its information security program. (NFR FY23-FISMA-08)

Recommendations:

RMA recommends the OCIO:

6. Implement the necessary oversight of RISCS to ensure that ISOs take action to review, update, and approve POA&Ms and RBDs, as necessary, before they become delinquent, taking into consideration the length of time required to obtain necessary approvals, and update RISCS. (NFR FY23-FISMA-08)
7. Ensure the system owners of the systems selected for testing address past due POA&Ms and RBDs. (NFR FY23-FISMA-08)

Further, RMA found that NASA did not have a formal process to document and implement lessons learned related to the Information Security Continuous Monitoring (ISCM) and Risk Management security domain areas. According to NASA officials, lessons learned activities were not performed because those activities were not incorporated within the Agency's policy and procedures. Without a formal, disciplined lessons learned process, NASA may not capture information from previous practice and actual responses to strengthen its security posture when addressing future events. (NFR FY23-FISMA-09)

Recommendation:

RMA recommends the OCIO:

8. Revise its policies and procedures to document and implement a lessons learned process based on risk events within the ISCM and Risk Management areas. System security

personnel should be instructed to record, analyze, and revise control activities to improve NASA's security posture. (NFR FY23-FISMA-09)

Supply Chain Risk Management: We determined NASA's overall maturity level for the Supply Chain Risk Management (SCRM) program was Consistently Implemented. NASA's Cybersecurity SCRM (C-SCRM) is intended to expose threats and vulnerabilities associated with products and services traversing the supply chain. Threats and vulnerabilities potentially compromise the confidentiality, integrity, or availability of an agency's systems and the information they contain.

NASA still has not incorporated enterprise-wide supplier risk evaluations into the Agency's continuous monitoring practices. However, NASA plans to complete the supplier risk evaluations by November 17, 2023. NASA faces increased supplier-related risks until enterprise-wide supplier risk evaluations are incorporated into the Agency's continuous monitoring practices. Specifically, adversaries may target and compromise weaknesses in the supply chain on both commercial off-the-shelf and custom information systems and components, leading to the denial, disruption, or degrading of the function of its systems. (NFR FY23-FISMA-05)

NASA has begun the process of developing its C-SCRM controls and has made measurable progress in developing and implementing its SCRM processes across the Agency. However, NASA had not completed its efforts to comply with the National Institute of Standards and Technology (NIST) SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, which lists controls required for an effective C-SCRM program. Specifically, NASA has not fully integrated its C-SCRM controls and processes across the Agency at the Enterprise (Level 1), Mission and Business Process (Level 2), and Operational (Level 3) levels and completed its implementation of the C-SCRM controls listed in Appendix A, *C-SCRM Security Controls*, of NIST 800-161. The controls are organized into 20 control families and are intended for agencies to implement across all three levels to ensure they have appropriately addressed its supply chain.

Development of a comprehensive C-SCRM program that includes the integration of processes and implementation of controls throughout an agency is a complex task that requires extensive effort and resources, given the multiple stakeholders and functional areas involved. In March 2022, NASA established a Supply Chain Security Working Group (SCSWG) to coordinate with Agency organizations to improve practices to adequately address the current and future threat environment impacting NASA's supply chain. The SCSWG established several goals to be accomplished in FY 2023 and beyond. Further, the OCIO has established two Enterprise processes, the Covered Article & Technology Supply Chain Assessment Needed (CATSCAN) and Proactive Supplier Engagement Process (PSEP), to assess agency suppliers' governance, cybersecurity, financial, geopolitical, and operational resilience risk posture. The PSEP was recognized as “best in class” by the National Cyber Director organization. The Agency's efforts are expected to continue through FY 2024.

Without integrated C-SCRM processes, the Agency is vulnerable to cybersecurity threats throughout the supply chain. In addition, there is an increased risk of compromised product integrity due to issues like tampering, counterfeiting, or unauthorized modifications. This can lead to reduced product quality, functionality, or reliability, impacting customer trust and satisfaction. (NFR FY23-FISMA-04)

Recommendations:

RMA recommends the OCIO:

9. Incorporate supplier risk evaluations into its continuous monitoring practices. (NFR FY23-FISMA-05)
10. Continue developing and implementing plans to integrate its C-SCRM controls and processes across the three Agency levels. (NFR FY23-FISMA-04)

PROTECT FUNCTION

The Protect Function relates to developing and implementing appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.[14] The domains included under this function are Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. We determined the Protect Function's maturity level was Consistently Implemented and not effective.

Configuration Management: We determined NASA's overall maturity level for the Configuration Management program was Consistently Implemented. NASA sets standard baselines for the operating system employed in its environment through its policies and procedures displayed on NASA's Security Configuration website. Further, NASA consistently utilized Security Content Automation Protocol validated software to scan all systems on its network for code-based and configuration-based vulnerabilities. NASA incorporated a lessons learned process into maintaining and updating its configuration specification policies and website. However, NASA did not have an effective process for the timely remediation of network vulnerabilities in its information technology environment in that NASA failed to apply software updates and security patches promptly. According to the *Cybersecurity Performance Metrics−All Assets* dashboard within NASA's Big Fix tracking system, as of June 6, 2023, 14% of Critical vulnerabilities and 40% of High vulnerabilities were overdue for remediation.[15]

Further, although NASA published standard baselines, the Agency failed to implement them at the information system level. Using NASA's Agency Cybersecurity Performance Metrics, which pulls information from the *BigFix Agency Security Configuration Settings* dashboard, RMA noted that 12% of the configuration baselines were not verified as implemented.[16]

[14] Ibid.

[15] Of a total of 279,517 vulnerabilities that were overdue, 40,271 were Critical (14%), 112,401 were High (40%), 125,760 were Medium (45%) and 1,085 were Low (1%). The total vulnerabilities include those from information systems with approved POA&Ms and RBDs.

[16] Of a total of 31,339,391 configuration baselines checked, 27,631,442 (88%) were verified and 3,707,949 (12%) were not verified.

NASA is transitioning to an enterprise model for monitoring and remediating vulnerabilities, enforcing the Agency's standard baselines, and moving away from Center-focused processes. Although the transition is not complete, NASA is adopting an approach in which the process will be centrally controlled. As processes are transitioned and the Agency Cybersecurity Executive Scorecard displays patch and configuration status in real time, the Agency is discovering inconsistencies between how Centers addressed patching and enforced baselines. Until the Agency resolves those issues and adopts consistent enterprise processes, their approach lacks entity-level control to assess and enforce the remediation of its vulnerabilities and enforcement of its baselines. Although the transition has shown increased communication and collaboration across the Agency, NASA continues to face an increased risk of compromises to its information security across the enterprise until the transition is more mature.

NASA's current process for remediation of network vulnerabilities and its use of nonstandard baselines increase the risk that mission information, IT assets or other sensitive data may be inadvertently or deliberately misused. Such misuse may result in improper information disclosure, manipulation, or theft. Additionally, vulnerabilities that are not corrected may lead to inappropriate or unnecessary changes to mission-focused information systems, which could result in the compromise of mission information or other sensitive data. (NFR FY23-FISMA-16)

Recommendation:

RMA recommends the OCIO:

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. (NFR FY23-FISMA-16)

Identity and Access Management: We determined NASA's overall maturity level for the Identity and Access Management program was Consistently Implemented. NASA managed its employees' and contractors' identity, credential, and access management (ICAM) protocols. NASA developed an Identification and Authentication policy to require multifactor authentication (MFA) for privileged and non-privileged users. MFA is a security measure that requires two or more proofs of identity before access is granted. MFA typically requires a combination of something the user knows (e.g., personal identification number, secret question), physically possesses (e.g., card, token), or inherently possesses (e.g., fingerprint, retina). NASA's policy defined their process for provisioning, managing, and reviewing privileged and non-privileged user accounts, that includes inventorying and conducting periodic reviews and adjustments for the privileged user accounts and permissions. The most common form of authentication is the use of Personal Identity Verification (PIV) cards and personal identification number. Further, NASA policies require MFA for local and remote access to its information systems and two-factor PIV card authentication is required for local access to non-privileged accounts.

Two of the four systems selected for testing as part of the FY 2023 evaluation had not instituted PIV card authentication or multifactor authentication for their non-privileged user accounts. Instead, the systems were accessed by the use of only a username and password. This was consistent with the FY 2022 evaluation, where the same issue was noted for one of the systems tested. Further, we found that 6 of 12 NASA business areas[17] had a user account PIV compliance rating. below 90.0%, ranging from 66.2% to 89.6%.

According to NASA officials, due to competing priorities, sufficient resources were not employed to fully comply with OMB M-11-11,[18] but its efforts are ongoing to provide all information systems with PIV-based multifactor authentication in lieu of username and password. Until PIV compliance is fully implemented throughout the Agency, NASA faces an increased risk of unauthorized access to its information system and data because usernames and passwords alone are not an effective control. This is a critical control because, without PIV-based multifactor authentication enforced at the application level, network users (either authorized or unauthorized) could gain access to applications they are not authorized to use, and public-facing systems could be susceptible to vulnerabilities and potential remote attacks. (NFR FY23-FISMA-15)

Recommendations:

RMA recommends the OCIO:

12. Continue the ongoing effort to enforce mandatory multifactor authentication using a NASA identity-based account and token from Agency ICAM service offerings (i.e., NASA PIV, Agency Smart Badge) for all information systems in NASA's environment. (NFR FY23-FISMA-15)
13. Ensure each information system owner of the systems selected for testing implements multifactor authentication for its non-privileged users. (NFR FY23-FISMA-15)

Data Protection and Privacy: We determined NASA's overall maturity level for the Data Protection and Privacy program was Consistently Implemented. NASA defined and communicated its policies and procedures for data exfiltration, enhanced network defenses, email authentication processes, and mitigation against Domain Name System (DNS) infrastructure tampering. Also, NASA consistently monitored inbound and outbound network traffic and ensured that all traffic passed through a web content filter that protects against phishing, and malware and blocks known malicious sites. NASA issued policies for designating, accessing, storing, disseminating, decontrolling, and destroying controlled unclassified information, including personally identifiable information (PII). The NASA OCIO also maintained security handbooks establishing processes to control and protect PII throughout the data lifecycle. NASA deployed a data loss prevention (DLP) capability within the Office 365 project. The DLP capability allowed NASA to identify, monitor, and respond to unencrypted sensitive information across NASA's network. However, NASA's ISCM strategy was missing the following NIST SP 800-53 control families introduced in Revision 5: Program Management (PM), PII Processing and Transparency (PT), and Supply Chain Risk Management (SR). Without including PM, PT, and SR controls in

[17] NASA business areas include nine centers, Headquarters, the Jet Propulsion Laboratory, and the NASA Shared Services Center.
[18] OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors* (February 3, 2011).

the ISCM Strategy, NASA cannot monitor or measure the effectiveness of its security controls, such as those meant for protecting PII and other agency-sensitive data. NASA may not be alerted to control weaknesses that, if not corrected, may lead to program management mismanagement concerns, privacy breaches, and compromises in the management of risk around its supply chain. See the Information Security Continuous Monitoring section below for the recommendation.

Security Training: We determined NASA's overall maturity level for the Security Training program was Managed and Measurable. The OCIO established and managed the IT Security Awareness and Training Center (ITSATC). ITSATC has existed since 1998 and develops, delivers, oversees, and enforces NASA's required annual IT security awareness training. ITSATC collaborates with stakeholders to provide and track cybersecurity awareness and specialized role-based training. RMA noted that roles and responsibilities were defined using roles from various Agency requirements. NASA has effectively used resources for stakeholders to consistently implement their security awareness training roles and responsibilities.

RMA found that NASA established and defined its security awareness and role-based training in one of its IT-HBKs, *Cybersecurity and Privacy Awareness, Training and Education* (ITS-HBK-2810.06-2B). NASA implemented a training awareness strategy. We found that NASA consistently tracked and kept records of users' completion of security training. In addition, NASA maintains quantitative and qualitative metrics to ensure the effectiveness of the training. RMA also noted that NASA implements an online security training platform to measure the progress of the users and then provides records and graphs to measure the effect. The training courses include insider threats, foreign travel, personal travel, telework, and data protection for different sensitivity levels in federal records management.

Further, NASA has addressed its identified knowledge, skills, and abilities gaps through talent acquisition. We reviewed the NASA Cybersecurity & Privacy Division (CSPD) workforce strategy. We noted that the CSPD workforce strategy maps the CSPD roles to the NIST's *National Initiative for Cybersecurity Education Framework*. CSPD implements Office of the Chief Human Capital Officer (OCHCO) Workforce policies and procedures for workforce assessment. NASA conducted an annual workforce plan to guide the direction and management of human capital within the Agency to ensure its missions are fully supported. We do not have recommendations to improve the Security Training Program.

DETECT FUNCTION

The Detect Function relates to the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events.[19] The domain included under this function is Information Security and Continuous Monitoring. We determined the Detect Function's maturity level was Defined and not effective.

[19] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

Information Security and Continuous Monitoring: We determined NASA's overall maturity level for the ISCM program was Defined.

NASA did not have a formal process to document and implement ISCM lessons learned to improve its existing control effectiveness. Without a formal, disciplined lesson-learned process, NASA may not capture information from previous practice, and actual responses to risk events are not used to strengthen NASA's security posture when addressing future events. See the Risk Management section above for the recommendation.

As noted in the Data Protection and Privacy section above, NASA's ISCM Strategy did not include the PM, PT, and SR control families introduced in Revision 5 of NIST SP 800-53. In addition, NASA's ISCM Strategy did not define its manual process of recording network devices in its NASA Manual Inventory (NMI) system. In response to our finding, NASA developed a corrective action plan with an estimated completion date of November 17, 2023.

During our FY 2023 FISMA evaluation, RMA was informed that NASA no longer had an ISCM Strategy because it had been withdrawn, so it could be updated to include the missing areas identified the previous year. RMA was informed the updates to NASA's ISCM Strategy are still in progress. In addition, NASA plans to update its ITS-HBK-AASTEP6. V.1.0.0, *Assessment and Authorization* Step *6: Monitor Policy* to more clearly specify the need to validate manual hardware inventory information in its continuous monitoring processes. Without a comprehensive ISCM Strategy, the Agency is unable to integrate all processes, metrics, and associated outputs to support decision making within its risk function. It cannot monitor or measure the effectiveness of its controls to obtain situation awareness across the Agency. Further, NASA may not be alerted to control weaknesses that, if not corrected, may lead to program mismanagement concerns, privacy breaches, and compromises in managing risk across the Agency. (NFR FY23-FISMA-13)

Further, in our FY 2022 FISMA evaluation, RMA found that two of the three operational systems selected for testing did not update their Authorization to Operate (ATO) and system-level Security Assessment Report (SAR) continuously or annually. In response to our finding, NASA developed a corrective action plan with an estimated completion date of November 17, 2023.

We found the same issue for two of the four systems selected for testing during the FY 2023 FISMA evaluation. One system, categorized as high-security information system, had an invalid ATO due to the following issues:

- The System Security Plan (SSP) did not include the results of a control assessment performed by an independent assessor. The controls in the SSP were self-assessed, but an independent assessment was required and had not been completed.
- The SSP lacked a SAR, and the implementation description statement for each NIST SP 800-53 Revision 5 control in the SSP did not clearly identify which of the four applications within the system that the self-assessment applied. In addition, although the controls found in the SSP indicated whether they had been assessed, there was no documentation supporting the self-assessment.

For the other system, categorized as a low-security information system, we identified the following issues:

- The ATO was overdue. The ATO was required to be done annually, and as of our evaluation on May 13, 2023, it had not been completed. The date of the latest ATO was March 6, 2022.
- The SAR was overdue. The independent SAR was required to be completed annually, and as of May 13, 2023, it had not been completed. The date of the latest SAR was January 12, 2022.

The Agency did not provide the resources needed to conduct the required independent assessment of controls, which led to the invalid ATO for the high-security information system. In addition, according to NASA management, ATOs and SARs were not updated timely due to an enterprise-wide reorganization and the conversion of policies and procedures to NIST SP 800-53 Revision 5. Management also stated that the many layers of review and approval required for ATOs and SARs caused delays in the approval process.

When ATOs are not updated and reviewed promptly, and an independent assessor does not conduct SARs, the overall risk exposure at NASA may be adversely impacted. Further, without an independent assessor, the assessment results would be considered insufficient to support the determination of security and privacy controls' existence and effectiveness of the controls. As a result, NASA may not be accurately measuring the Agency's risks related to information security. (NFR FY23-FISMA-06)

Recommendations:

RMA recommends the OCIO:

14. Develop and implement an ISCM Strategy in accordance with OMB Circular No. A-130, *Managing Information as a Strategic Resource*, and NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, including defining metrics, status monitoring frequencies, and control assessment frequencies. (NFR FY23-FISMA-13)
15. Ensure that the security controls in control families PM, PT, and SR are updated and defined within the Agency's ISCM strategy. (NFR FY23-FISMA-13)
16. Document the NMI 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. (NFR FY23-FISMA-13)
17. Implement the necessary oversight to monitor RISCS for delinquent or invalid ATOs and SARs so that RISCS provides sufficient information to determine NASA's risk exposure. (NFR FY23-FISMA-06)
18. Ensure ATOs and SARs are properly completed for the systems selected for testing. (NFR FY23-FISMA-06)
19. Ensure each information system owner of the systems selected for testing (1) updates the SSP to specify the specific application associated with the implementation statement for

each NIST SP 800-53 Revision 5 control, and (2) has the system controls assessed by an independent assessor. (NFR FY23-FISMA-06)

RESPOND FUNCTION

The Respond Function relates to developing and implementing appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.[20] The domain included under this function is Incident Response. We determined the Respond Function's maturity level was Consistently Implemented and not effective.

Incident Response: We determined NASA's overall maturity level for the Incident Response program was Consistently Implemented. NASA consistently implemented its policies, procedures, and incident detection and analysis processes. NASA established an Incident Response Plan that provided a detailed description of incident handling, defined common threat vectors for classifying incidents, defined its processes for detecting, analyzing, and prioritizing incidents, and outlined response steps to security events or incidents. NASA's ITS-HBK, *Information Security Incident Management (CUI)* (ITS-HBK-2810.09-02A), provided information detailing NASA's incident detection and analysis and accompanying procedures. NASA used several tools and technologies to detect anomalies and monitor baseline network traffic. NASA established a mature process for Agency incident handling. The NASA Information Security Incident Response Standard Operating Procedures defined incident containment strategies for each key incident type, provided a detailed description of incident handling, defined common threat vectors for classifying incidents, provided its processes for detecting, analyzing, and prioritizing incidents, and outlined response steps.

RMA found that NASA did not meet the Event Logging (EL) requirements at the EL2 (intermediate) maturity level in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. NASA was required to reach EL2 maturity within 18 months after the issuance of M-21-31, which was issued on August 27, 2021.

NASA did not meet the EL2 logging requirements level due to the complexity and comprehensiveness of logging requirements. Those requirements necessitate that an agency as dispersed as NASA needs to capture, retain, and manage an extensive catalog of logging records to meet the required compliance. In addition, NASA was working on a cost-effective solution to meet multiple OMB memorandums from Executive Order 14028, *Improving the Nation's Cybersecurity*, which caused the prioritization of other projects, which then precipitated the delay in addressing the complexities required to fulfill the logging requirements of M-21-31. By not meeting the logging requirements at maturity level EL2 (intermediate), NASA decreases its ability to ensure the highest-level security operations center and accelerate incident response efforts to enable more effective defense of federal information. (NFR FY23-FISMA-07)

[20] Ibid.

Recommendation:

RMA recommends the OCIO:

20. Continue its efforts to prioritize projects that address the complexities required across EL tiers to meet the intermediate (EL2) maturity level in accordance with OMB M-21-31. (NFR FY23-FISMA-07)

RECOVER FUNCTION

The Recover Function relates to developing and implementing appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident.[21] The domain included under this function is Contingency Planning. We determined the Recover Function's maturity level was Defined and not effective.

Contingency Planning: We determined NASA's overall maturity level for the Contingency Planning program was Defined. NASA defined the processes for conducting system-level Business Impact Analysis (BIA) and testing contingency plans.

In our FY 2022 FISMA evaluation, RMA found one of the three operational systems selected for testing did not perform a BIA, which analyzes the system's requirements, functions, interdependencies, and priorities to minimize the impact of an event of significant disruption. In response to the FY 2022 finding, NASA developed a corrective action plan with an estimated completion date of November 17, 2023.

During our FY 2023 FISMA evaluation, we found that one of the four systems selected for testing did not perform a BIA. NASA lacks centralized IT governance procedures or oversight to monitor and enforce BIA compliance at the system level. There is no effective process to ensure that systems in RISCS, the system of record, have current BIAs. Without a current system-level BIA, system personnel may not prioritize recovery operations effectively in a service-impacting incident. (NFR FY23-FISMA-14)

In addition, contingency plans for two information systems were not tested as required by NASA's ITS-HBK, *Contingency Planning* (ITS-HBK-2810.08-01A). Specifically, for one information system the contingency plan was last tested in September 2017, although it should have been tested annually. Upon RMA notifying the information system owner, system personnel provided an updated contingency plan in April of 2023; however, this plan had not been tested. For the second system, the contingency plan was created in March 2023, but an initial test to confirm the accuracy of recovery procedures and the overall effectiveness of the plan was not conducted.

NASA did not implement the necessary oversight and/or enforcement mechanisms and controls to ensure all system-level contingency plans were developed, tested, and results reviewed to develop

[21] Ibid.

corrective actions, as needed, to strengthen the effectiveness of each contingency plan. Contingency plan testing is critical to ensuring effective plans are in place. Without effective system contingency plans, NASA's mission data is at a higher risk of loss due to an unscheduled disruption. (NFR FY23-FISMA-12)

Further, an external information system did not have an Interconnection Security Agreement (ISA) in place to specify the technical and security requirements of the interconnection with its external system partner. An ISA defines the purpose of the interconnection, identifies the relevant authorities, specifies the responsibilities of NASA and its external partner, and defines the terms of the agreement.

NASA did not implement the necessary oversight and/or enforcement mechanisms to ensure all external information systems had ISAs in place to define how each entity would manage, operate, use, and secure the interconnection between NASA and its external partners. Without an ISA between NASA and its external information system partners, NASA-owned data collected, stored, and/or transmitted in the partner's environment may not receive adequate and appropriate confidentiality, integrity, and availability protections. (NFR FY23-FISMA-11)

<u>Recommendations</u>:

RMA recommends the OCIO:

21. Design and implement the necessary entity-wide oversight, enforcement mechanisms, and controls to ensure all system-level BIAs are accurate and reviewed annually. (NFR FY23-FISMA-14)
22. Review all information systems to determine if a BIA has been performed in accordance with NASA policy. (NFR FY23-FISMA-14)
23. Ensure each information system owner of the systems selected for testing performs and completes a system-level BIA. (NFR FY23-FISMA-14)
24. Implement the necessary oversight to monitor RISCS for delinquent testing of contingency plans. (NFR FY23-FISMA-12)
25. Ensure each information system owner of the systems selected for testing conducts a test of its contingency plan annually. (NFR FY23-FISMA-12)
26. Ensure each information system owner of the systems selected for testing confirms the adequacy of its recovery procedures and the plan's overall effectiveness. (NFR FY23-FISMA-12)
27. Ensure that each information system owner of external systems has a current ISA that defines how each entity will manage, operate, use, and secure the interconnection. (NFR FY23-FISMA-11)

Results Summary

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we concluded that NASA's information security program and practices were consistently implemented. They were maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. However, we found that NASA's information security program and practices were not effective for the period October 1, 2022, through May 31, 2023, since the overall maturity level of NASA's information security program was Consistently Implemented.

Objective, Scope, and Methodology

The objective of this evaluation was to assess the effectiveness of NASA's information security program and practices for the period October 1, 2022, through May 31, 2023.

NASA's information system infrastructure comprises office networks or applications and several system service providers. RMA assessed NASA against the FY 2023 core and supplemental metrics for four selected systems (**Table 4**).

Table 4: RMA's Selection of NASA Systems for FY 2023

#	System Name	Location	FIPS 199 Categorization
	Internal and External Systems		
1	MSFC Medical Systems	Internal	High
2	GRC Institutional Monitoring Control Systems	Internal	Moderate
3	Psionic Support Systems	External	Moderate
4	UAH/ITSC End User Devices	External	Low

RMA evaluated the effectiveness of NASA's information security program and practices in accordance with CIGIE's *Quality Standards for Inspection and Evaluation* (Blue Book) (December 2020), requirements set forth by NASA, NIST, OMB, and as outlined in the *FY 2023 – 2024 IG FISMA Reporting Metrics*. The Blue Book provides a solid framework for inspection and evaluation work by OIG. It provides a flexible and effective mechanism for oversight and empowers inspection, evaluation, and multidisciplinary staff to produce timely, credible reports to improve agency operations. We assessed NASA's effectiveness in accordance with Blue Book standards. The *FY 2023 – 2024 IG FISMA Reporting Metrics* are aligned with five Cybersecurity Functions (key performance areas) within NIST's Cybersecurity Framework as follows:

- **Identify**, which includes questions pertaining to risk management and supply chain risk management;
- **Protect**, which includes questions pertaining to configuration management, identity and access management, data protection and privacy, and security training;
- **Detect**, which includes questions pertaining to information security continuous monitoring;
- **Respond**, which includes questions pertaining to incident response; and
- **Recover**, which includes questions pertaining to contingency planning.

To perform our evaluation of NASA's information security program and practices, RMA considered NIST SP 800-53A Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*; NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; FISMA guidance from CIGIE, OMB, and DHS; and NASA policies and procedures.

To adhere to changes in the scoring methodology described in the *FY 2023 – 2024 IG FISMA Reporting Metrics*, we determined the maturity level for each of the nine domains by using a calculated average approach, in which we took the average of the metrics in a domain to determine the effectiveness of the individual function areas and overall program.[22] Core metrics and supplemental metrics were averaged independently to determine a domain's maturity calculation and provided data points for the assessed program and function effectiveness. RMA understands that the objective for these changes was to provide IGs additional flexibility because the calculated averages will not automatically be rounded to a particular maturity level. IGs are now encouraged to focus on the results of the core metrics and that the calculated averages of the supplemental metrics be used as data points to support the determination of the overall program and function level of effectiveness.

Criteria

We focused our FISMA evaluation approach on the federal information security guidelines that NASA, NIST, and OMB developed. NIST SPs provide guidelines considered essential to developing and implementing NASA security programs. The following is a listing of the criteria used in the performance of the FY 2023 FISMA evaluation.

NIST Federal Information Processing Standards (FIPS), SPs, and Other Guidance

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*

[22] DHS, *FY 2023 – 2024 Inspector General FISMA Reporting Metrics* (February 10, 2023), page 8.

- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- NIST SP 800-63, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments, Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments, Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- OMB Circular No. A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*

- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High-Value Assets*
- OMB Memorandum M-16-17, *OMB Circular No. A-123*, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*

DHS's CISA

- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
- Binding Operational Directive 18-02, *Securing High Value Assets*
- Binding Operational Directive 18-01, *Enhance Email and Web Security*
- Binding Operational Directive 17-01, *Removal of Kaspersky-Branded Products*
- Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*
- Emergency Directive 22-03, *Mitigate VMWare Vulnerabilities*
- Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*

- Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*
- Emergency Directive 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- Emergency Directive 20-03, *Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday*
- Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*

NASA Policies

- ITS-HBK-2810.02-05A, *Security Assessment and Authorization: External Information Systems*
- ITS-HBK-2810.03-02B, *Planning*
- ITS-HBK-2810.04-01A, *Security Categorization, Risk Assessment, Vulnerability*
- ITS-HBK-2810.05-02B, *System and Service Acquisition*
- ITS-HBK-2810.06-02B, *Cybersecurity and Privacy Awareness, Training and Education*
- ITS-HBK-2810.07-02B, *Configuration Management*
- ITS-HBK-2810.08-01A, *Contingency Planning*
- ITS-HBK-2810.09-02A, *Information Security Incident Management (CUI)*
- ITS-HBK-2810.11-2C, *Media Protection and Sanitization*
- ITS-HBK-2810.12-02B, *Physical and Environmental Protection*
- ITS-HBK-2810.14-03D, *System and Information Integrity*
- ITS-HBK-2810.15-01A, *Access Control*
- ITS-HBK-2810.16-02B, *Audit and Accountability*
- ITS-HBK-2810.17-02B, *Identification and Authentication*
- ITS-HBK-2810.18-02B, *System and Communications Protection*
- ITS-HBK-2841-03A, *Identity, Credential, and Access Management (ICAM) Services*
- ITS-HBK-AASTEP2. V.1.0.0, *Assessment and Authorization Step-2: Select Policy*
- ITS-HBK-AASTEP5. V.1.0.0, *Assessment and Authorization Step 5: Authorize Policy*
- ITS-HBK-AASTEP6. V.1.0.0, *Assessment and Authorization Step 6: Monitor Policy*
- ITS-HBK-CUI_v1.0.0, *Controlled Unclassified Information Handbook*
- ITS-HBK-SCRM. 2810.v1.0.0, *Information & Communications Technology Supply Chain Risk Management (ICT SCRM)*
- NASA Procedural Requirements (NPR) 2810.1F, *Security of Information and Information Systems*
- NASA Technical Specification – NASA – SPEC – 2661.ODVr5 v1.2, *NASA's Organization-Defined Values for NIST Special Publication 800 – 53 Revision 5*

Acronyms

ATO	Authorization To Operate
BIA	Business Impact Analysis
CATSCAN	Covered Article & Technology Supply Chain Assessment Needed
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
C-SCRM	Cybersecurity Supply Chain Risk Management
CSIP	Cybersecurity Strategy and Implementation Plan
CSPD	Cybersecurity & Privacy Division
CUI	Controlled Unclassified Information
DHS	U.S. Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name System
EL	Event Logging
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	U.S. Government Accountability Office
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ICT SCRM	Information & Communications Technology Supply Chain Risk Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
IT	Information Technology
ITSATC	IT Security Awareness and Training Center
ITSC	Information Technology and Systems Center
ITS-HBK	Information Technology Security Handbook
MFA	Multifactor Authentication
NASA	National Aeronautics and Space Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NMI	NASA Manual Inventory
NPR	NASA Procedural Requirements
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PM	Program Management

POA&M	Plan of Actions and Milestones
PSEP	Proactive Supplier Engagement Process
PT	PII Processing and Transparency
RBD	Risk Based Decision
RISCS	Risk Information Security Compliance System
RMA	RMA Associates, LLC
SAR	Security Assessment Report
SCRM	Supply Chain Risk Management
SCSWG	Supply Chain Security Working Group
SP	Special Publication
SR	Supply Chain Risk Management
SSDF	Secure Software Development Framework
SSP	System Security Plan
TIC	Trusted Internet Connection

Appendix A – NASA OIG FY 2023 IG CyberScope Submission

The Appendix A contents labeled "For Official Use Only" on pages 28 through 66 are not being publicly released.

Appendix B – Status of Prior Year Recommendations

Table 5 provides the status of prior FISMA evaluation recommendations as of May 31, 2023.

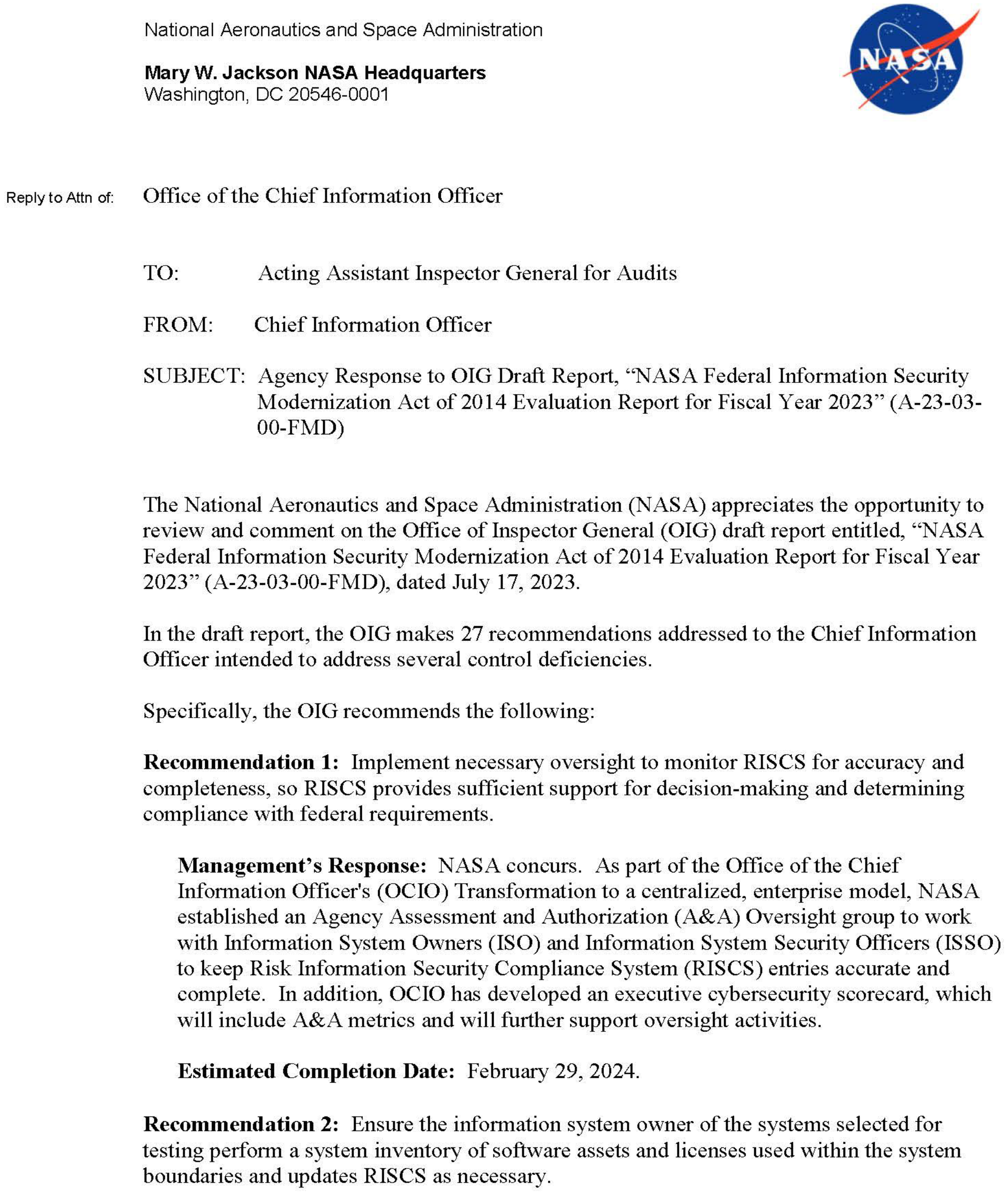
Table 5: Status of FY 2022 FISMA Evaluation Recommendations

Report and Recommendation No.	Recommendations	Status
IG-23-006, Re 1	Implement the necessary entity-wide oversight to monitor RISCS for delinquent ATOs and SARs and ensure the information system owners of the systems selected for testing in this evaluation complete delinquent ATOs and SARs so RISCS provides sufficient information to determine NASA's risk exposure.	Repeat – Please refer to the FY 2023 Recommendations 17 and 18 in the Detect section above.
IG-23-006, Rec 2	Design and implement the necessary entity-wide oversight, enforcement mechanisms, and controls to ensure all system-level BIAs are accurate and reviewed annually, as well as ensure the information system owners of the systems selected for testing in this evaluation complete a system-level BIA.	Repeat – Please refer to the FY 2023 Recommendations 21 and 23 in the Recover section above.
IG-23-006, Rec 3	Review all information systems to determine if a BIA has been performed in accordance with NASA's Information Technology Security Handbook (ITS-HBK), *Contingency Planning* (ITS-HBK-2810.08-01A).	Repeat – Please refer to the FY 2023 Recommendation 22 in the Recover section above.
IG-23-006, Rec 4	Implement the necessary entity-wide oversight to monitor RISCS for accuracy and completeness, including reviewing portfolio-wide reports or dashboards demonstrating compliance with federal requirements and enhancing decision-making.	Repeat – Please refer to the FY 2023 Recommendation 1 in the Identify section above.
IG-23-006, Rec 5	Design and implement the necessary entity-wide oversight enforcement mechanisms and ensure the information system owner of the system selected for testing during this evaluation perform a system inventory of its software assets and licenses to ensure all software and license information are accurate and reviewed annually.	Repeat – Please refer to the FY 2023 Recommendations 2 and 3 in the Identify section above.

Report and Recommendation No.	Recommendations	Status
IG-23-006, Rec 6	Develop policies, procedures, and processes to manage the cybersecurity risks of risk framing, risk response, and risk monitoring in accordance with NASA policy.	Repeat – Please refer to the FY 2023 Recommendation 4 in the Identify section above.
IG-23-006, Rec 7	Document the NMI process in NASA's ISCM Strategy to ensure its hardware inventory monitoring process is accurate, complete, and fully aligned with NASA's other continuous monitoring guidance.	Repeat – Please refer to the FY 2023 Recommendation 16 in the Detect section above.
IG-23-006, Rec 8	Develop a policy and implement the necessary entity-wide oversight to monitor risk through a risk register and a risk profile to provide enterprise-wide metrics to inform top management of its IT risks.	Repeat – Please refer to the FY 2023 Recommendation 5 in the Identify section above.
IG-23-006, Rec 9	Implement the necessary oversight to monitor POA&Ms and RBDs in RISCS to identify ones that require action so it can ensure that the ISOs take the necessary action to review, update, and approve POA&Ms and RBDs, as necessary, before they become delinquent, taking into consideration the length of time required to obtain necessary approvals, and update RISCS.	Repeat – Please refer to the FY 2023 Recommendation 6 in the Identify section above.
IG-23-006, Rec 10	Ensure that the system owners of the systems selected for testing in this evaluation address its past due POA&Ms and unapproved RBDs.	Repeat – Please refer to the FY 2023 Recommendation 7 in the Identify section above.
IG-23-006, Rec 11	Ensure that the system owner of the system selected for testing in this evaluation addresses its unapproved RBD.	Repeat – Please refer to the FY 2023 Recommendation 7 in the Identify section above.

Report and Recommendation No.	Recommendations	Status
IG-23-006, Rec 12	Incorporate supplier risk evaluations into its continuous monitoring practices outlined in NASA's ISCM Strategy.	Repeat – Please refer to the FY 2023 Recommendation 9 in the Identify section above.
IG-23-006, Rec 13	Increase its resources and effort to enforce MFA using a NASA Identify-based account and token from Agency ICAM service offerings (i.e., NASA PIV, Agency Smart Badge) for all moderate and high information systems in NASA's environment to comply with NASA, NIST, and OMB's guidelines.	Repeat – Please refer to the FY 2023 Recommendation 12 in the Protect section above.
IG-23-006, Rec 14	Ensure the information system owner of the system selected for testing during this year's evaluation implement PIV or Phishing Resistant MFA for its non-privileged users to comply with NASA, NIST, and OMB's guidelines.	Repeat – Please refer to the FY 2023 Recommendation 13 in the Protect section above.
IG-23-006, Rec 15	Ensure the security controls for protecting PII and other agency-sensitive data throughout the data lifecycle found in control families PM, PT, and SR are updated and defined within the Agency's ISCM strategy.	Repeat – Please refer to the FY 2023 Recommendation 15 in the Detect section above.
IG-23-006, Rec 16	Establish and implement policies and procedures to periodically update its cybersecurity workforce assessment.	Closed
IG-23-006, Rec 17	Revise its ISCM policies to document and implement lessons learned based on risk events whereby employees are instructed to record, analyze, and revise control activities to improve NASA's security posture.	Repeat – Please refer to the FY 2023 Recommendation 8 in the Identify section above.

Appendix C – Management Response



National Aeronautics and Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001

Reply to Attn of: Office of the Chief Information Officer

TO: Acting Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, "NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023" (A-23-03-00-FMD)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023" (A-23-03-00-FMD), dated July 17, 2023.

In the draft report, the OIG makes 27 recommendations addressed to the Chief Information Officer intended to address several control deficiencies.

Specifically, the OIG recommends the following:

Recommendation 1: Implement necessary oversight to monitor RISCS for accuracy and completeness, so RISCS provides sufficient support for decision-making and determining compliance with federal requirements.

> **Management's Response:** NASA concurs. As part of the Office of the Chief Information Officer's (OCIO) Transformation to a centralized, enterprise model, NASA established an Agency Assessment and Authorization (A&A) Oversight group to work with Information System Owners (ISO) and Information System Security Officers (ISSO) to keep Risk Information Security Compliance System (RISCS) entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.
>
> **Estimated Completion Date:** February 29, 2024.

Recommendation 2: Ensure the information system owner of the systems selected for testing perform a system inventory of software assets and licenses used within the system boundaries and updates RISCS as necessary.

Management's Response: NASA concurs. The OCIO's Federal Information Security Modernization Act of 2014 (FISMA) oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that focus areas, such as performing a system inventory of software assets and licenses and updating RISCS, are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 3: Implement necessary oversight to monitor RISCS for accuracy and completeness of software and license information.

Management's Response: NASA concurs. As part of the OCIO's Transformation to a centralized, enterprise model, we established an A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: February 29, 2024.

Recommendation 4: Continue its efforts in developing policies, procedures, and processes for risk framing, risk response, and risk monitoring.

Management's Response: NASA concurs. OCIO's Enterprise Cybersecurity Risk Management (ECRM) team has been working on establishing the fundamental elements of an ECRM program and will continue to mature the program, including developing policies, procedures, and processes for risk framing, risk response, and risk monitoring.

Estimated Completion Date: February 29, 2024.

Recommendation 5: Continue its efforts to develop and implement the necessary entity-wide oversight policy and procedures to monitor risk through a risk register and a risk profile that provide enterprise-wide metrics to inform top management of its Information Technology (IT) risks.

Management's Response: NASA concurs. OCIO's ECRM team has been working on establishing the fundamental elements of an ECRM program and will continue to mature the program, including developing policies and procedures to monitor risk through a risk register and a risk profile.

Estimated Completion Date: February 29, 2024.

Recommendation 6: Implement the necessary oversight of RISCS to ensure that ISOs take action to review, update, and approve POA&Ms and RBDs, as necessary, before they become delinquent, taking into consideration the length of time required to obtain necessary approvals, and update RISCS.

Management's Response: NASA concurs**.** As part of the OCIO's Transformation to a centralized, enterprise model, we established an A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: February 29, 2024.

Recommendation 7: Ensure the system owners of the systems selected for testing address past due POA&Ms and RBDs.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that focus areas, such as past-due Plans of Actions and Milestones (POAMs) and Risk Based Decisions (RBDs), are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 8: Revise its policies and procedures to document and implement a lessons-learned process based on risk events within the ISCM and Risk Management areas. System security personnel should be instructed to record, analyze, and revise control activities to improve NASA's security posture.

Management's Response: NASA concurs. As part of OCIO's Transformation, an A&A oversight group has been established and a new A&A Strategy Lead role was created and filled. Additionally, OCIO's ECRM team has been working on establishing the fundamental elements of an ECRM program. As these groups mature, they will establish a process for incorporating lessons learned into Information Security Continuous Monitoring (ISCM) and risk management policies and procedures after risk events.

Estimated Completion Date: February 29, 2024.

Recommendation 9: Incorporate supplier risk evaluations into its continuous monitoring practices.

Management's Response: NASA concurs. NASA maintains one of the most developed Supply Chain Risk Management (SCRM) programs in the Federal government and routinely performs evaluations of supplier risks of all criticalities. However, NASA will review its continuous monitoring guidance and practices to see how supplier risk evaluations may be best included.

Estimated Completion Date: February 29, 2024.

Recommendation 10: Continue developing and implementing plans to integrate its C-SCRM controls and processes across the three Agency levels.

Management's Response: NASA concurs. OCIO will continue to lead and support Enterprise Supply Chain efforts across the Agency including the Supply Chain Security Working Group and Supply Chain Resiliency Board.

Estimated Completion Date: July 31, 2024.

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.

Management's Response: NASA concurs. NASA is currently transitioning away from Center-focused processes to an enterprise model for monitoring and remediating vulnerabilities and enforcing the Agency's standard baselines. Although the transition is not complete, NASA is adopting an approach in which the monitoring and enforcement process will be centrally controlled.

Estimated Completion Date: July 31, 2024.

Recommendation 12: Continue the ongoing effort to enforce mandatory multifactor authentication using a NASA identity-based account and token from Agency ICAM service offerings (i.e., NASA PIV, Agency Smart Badge) for all information systems in NASA's environment.

Management's Response: NASA concurs. OCIO is continuing work on multiple efforts to increase Personal Identity Verification (PIV) card use and enforcement across the enterprise. In addition, OCIO has developed an executive cybersecurity scorecard to help focus management attention at all levels to increase the use of PIV wherever possible.

Estimated Completion Date: February 29, 2024.

Recommendation 13: Ensure each information system owner of the systems selected for testing implements multifactor authentication for its non-privileged users.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that focus areas such as the implementation of multifactor authentication for non-privileged users are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 14: Develop and implement an ISCM Strategy in accordance with OMB Circular No. A-130, *Managing Information as a Strategic Resource, and NIST SP 800-137A, Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, including defining metrics, status monitoring frequencies, and control assessment frequencies.

Management's Response: NASA concurs. NASA is working toward the development of this strategy in response to the Fiscal Year (FY) 2022 finding and will continue to develop and implement this strategy in the year ahead.

Estimated Completion Date: February 29, 2024.

Recommendation 15: Ensure that the security controls in control families PM, PT, and SR are updated and defined within the Agency's ISCM strategy.

Management's Response: NASA concurs. NASA is working toward the development of this strategy in response to the FY 2022 finding and will continue to develop and implement this strategy in the year ahead. This strategy will include the NIST SP 800-53 Rev 5 control families Program Management (PM), personally identifiable information Processing and Transparency (PT), and Supply Chain Risk Management (SR) as noted in the draft report.

Estimated Completion Date: February 29, 2024.

Recommendation 16: Document the NMI 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.

Management's Response: NASA concurs. NASA is working toward the development of this strategy in response to the FY 2022 finding and will continue to develop and implement this strategy in the year ahead. This strategy will include the definition of recording network devices in the NASA Manual Inventory system.

Estimated Completion Date: February 29, 2024.

Recommendation 17: Implement the necessary oversight to monitor RISCS for delinquent or invalid ATOs and SARs so that RISCS provides sufficient information to determine NASA's risk exposure.

Management's Response: NASA concurs. As part of the OCIO's Transformation to a centralized, enterprise model, we established an Agency A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: February 29, 2024.

Recommendation 18: Ensure ATOs and SARs are properly completed for the systems selected for testing.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that focus areas such as Authorization to Operate (ATO) updates and Security Assessment Reports are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 19: Ensure each information system owner of the systems selected for testing (1) updates the SSP to specify the specific application associated with the implementation statement for each NIST SP 800-53 Revision 5 control, and (2) has the system controls assessed by an independent assessor.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that focus areas, such as System Security Plan updates and Independent Assessments, are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 20: Continue its efforts to prioritize projects that address the complexities required across EL tiers to meet the intermediate (EL2) maturity level in accordance with OMB M-21-31.

Management's Response: NASA concurs. NASA's OCIO is facilitating the development of a comprehensive plan to address all three Event Logging (EL) tiers, with a specific emphasis on meeting the requirements for EL2. As part of our commitment to enhancing our cybersecurity posture, the NASA OCIO will continue to prioritize projects that address the complexities and demands across all EL tiers. This initiative aligns with our interpretation of M-21-31, aiming to ensure all components satisfy the requirements for Intermediate Logging Categories, Publication of Standardized Log Structure, Inspection of Encrypted Data, and Intermediate Centralized Access.

Estimated Completion Date: July 31, 2024.

Recommendation 21: Design and implement the necessary entity-wide oversight, enforcement mechanisms, and controls to ensure all system-level BIAs are accurate and reviewed annually.

Management's Response: NASA concurs. Part of the recent OCIO Transformation to a centralized, enterprise model was the establishment of a consolidated Agency A&A Oversight group that will be able to determine which systems may lack a Business Impact Analysis (BIA). OCIO has also developed an executive cybersecurity scorecard which will include A&A metrics to further support oversight activities.

Estimated Completion Date: February 29, 2024.

Recommendation 22: Review all information systems to determine if a BIA has been performed in accordance with NASA policy.

Management's Response: NASA concurs. As part of the OCIO's Transformation to a centralized, enterprise model, NASA established an Agency A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: February 29, 2024.

Recommendation 23: Ensure each information system owner of the systems selected for testing performs and completes a system-level BIA.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that FISMA focus areas, such as a completed BIA, are addressed.

Estimated Completion Date: February 29, 2024.

Recommendation 24: Implement the necessary oversight to monitor RISCS for delinquent testing of contingency plans.

Management's Response: NASA concurs. As part of the OCIO's Transformation to a centralized, enterprise model, NASA established an Agency A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. In addition, OCIO has developed an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: July 31, 2024.

Recommendation 25: Ensure each information system owner of the systems selected for testing conducts a test of its contingency plan annually.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that FISMA focus areas, such as contingency plan testing, are addressed.

Estimated Completion Date: July 31, 2024.

Recommendation 26: Ensure each information system owner of the systems selected for testing confirms the adequacy of its recovery procedures and the plan's overall effectiveness.

Management's Response: NASA concurs. The OCIO's FISMA oversight team is developing a checklist for the owners of systems selected for testing by the OIG that will help ensure that FISMA focus areas, such as recovery procedures and plan effectiveness, are addressed.

Estimated Completion Date: July 31, 2024.

Recommendation 27: Ensure that each information system owner of external systems has a current ISA that defines how each entity will manage, operate, use, and secure the interconnection.

Management's Response: NASA concurs. As part of the OCIO's Transformation to a centralized, enterprise model, NASA established an A&A Oversight group to work with ISO and ISSO to keep RISCS entries accurate and complete. This group will provide (through its A&A oversight role) additional scrutiny on NASA's external systems to ensure Interconnection Security Agreements are included where needed.

Estimated Completion Date: July 31, 2024.

We have reviewed the report/draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Matthew DeGrave at (757) 864-6838.

JEFFREY
SEATON

Digitally signed by
JEFFREY SEATON
Date: 2023.08.11
11:44:20 -04'00'

Jeff Seaton
Chief Information Officer