NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

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

December 19, 2022

TO: Jeff Seaton
Chief Information Officer

SUBJECT: Final Report, *NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022* (Report No. IG-23-006; Assignment No. A-22-11-00-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 2022 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 agency cybersecurity programs are required to meet to be considered 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 Kimberly F. Benoit, Assistant Inspector General for Audits, at 202-358-0378 or kimberly.f.benoit@nasa.gov, if you have any questions about the enclosed report.

Paul K. Martin
Inspector General

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

Enclosure—1

RMA Associates
Auditors. Consultants. Advisors.

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

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

Evaluation Report for Fiscal Year 2022

RMA | Associates
Auditors. Consultants. Advisors.

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

December 15, 2022

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 2022.

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) 2022. The objective of this evaluation was to evaluate the effectiveness of NASA's information security program and practices for the period October 1, 2021, through September 30, 2022. 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.

Beginning with the FY 2022 FISMA period, the Office of Management and Budget identified 20 Core Inspector General Metrics (FY 2022 Core IG Metrics) in its *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, of which IGs were required to assess the maturity levels. As part of our evaluation, we evaluated the FY 2022 Core IG Metrics. We assessed the maturity levels on behalf of NASA's Office of Inspector General, as shown in Appendix A. These metrics provide reporting requirements across functional areas to be addressed in the independent assessment of agencies' information security programs.

In summary, we found NASA's information security program and practices were not effective for the period October 1, 2021 through September 30, 2022.

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

RMA Associates
Auditors. Consultants. Advisors.

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

Table of Contents

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

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. 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 Department of Homeland Security (DHS) for the collection of annual FISMA responses.

NASA's Office of Inspector General (OIG) engaged RMA to conduct an 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, 2021, through September 30, 2022.

As part of our evaluation, we responded to the fiscal year (FY) 2022 Core Inspector General Metrics (FY 2022 Core IG Metrics) specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (issued on April 13, 2022). We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards. Our responses to the 20 FY 2022 Core IG Metrics, which align with questions from DHS's *FY 2021 Inspector General FISMA Reporting Metrics Version 1.1* (May 12, 2021), are provided in Appendix A, NASA OIG 2022 IG CyberScope Submission. These core metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs. See Objective, Scope, and Methodology for more detail. We also considered applicable OMB policy and guidelines, and NIST standards and guidelines.

Summary Evaluation Results

We concluded that consistent with applicable FISMA requirements, OMB policy, guidance, and NIST standards and guidelines, NASA's information security program and practices were established and maintained for the five Cybersecurity Functions[2] and nine FISMA Metric Domains.[3] The overall maturity level of NASA's information security program was determined as Consistently Implemented (Level 3), as described in this report. Within the context of the FISMA maturity model, Level 4, Managed and Measurable, represents an effective level of security. As

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (December 18, 2014).
[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The nine FISMA Metric Domains were aligned with the five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.
[3] As described in the FISMA Reporting Metrics, the nine FISMA Metric Domains 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.

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

such, we found NASA's information security program and practices were not effective for the period October 1, 2021, through September 30, 2022.

We provided NASA with a draft of this report for comment. NASA concurred on 15 recommendations, partially concurred on one recommendation, and non-concurred on one other. After carefully considering the information provided by NASA, we did not revise our 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, our solar system, and beyond. NASA conducts research, testing, and development to advance aeronautics, including electric propulsion and supersonic flight. 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 (STEM) 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 requires 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 the Federal Information Security Modernization Act of 2014 (FISMA), which amended FISMA 2002 and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes result

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

in less overall reporting, strengthen the use of continuous monitoring in systems, increased focus on the agencies for compliance, and produce 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 assessments' 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 provides OMB oversight authority of agency security policies and practices and provides authority for implementing agency policies and practices for information systems to DHS.[4]

FISMA requires 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

[4] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (December 2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521.

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

threat, vulnerability, or risk. It authorizes the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[5]

FISMA "directs the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards."[6]

Additionally, FISMA directs Federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the U.S. Government Accountability Office (GAO). Reports are required to include: (1) threats and threat factors, vulnerabilities, and impacts; (2) risk assessments of affected systems before and the status of compliance of the systems at the time of major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[7]

Key Changes to the FY 2022 IG FISMA Metrics

One of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. OMB issued Memorandum M-22-05,[8] which provides guidance on Federal information security and privacy management requirements. OMB Office of the Federal Chief Information Officer published *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, which is geared to the President's Management Agenda, on April 13, 2022. The metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the Intelligence Community. Research, interviews, and IG survey data provided quantitative and qualitative information to formulate these guidelines. The core metrics consist of 20 of 66 FISMA questions from the *FY 2021 IG FISMA Reporting Metrics v1.1*, May 2021. The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity.

OMB Memorandum M-22-05 adjusted the timeline for the IG evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the IG's evaluation of agency effectiveness finished in October. However, for FY 2022 the IG evaluation timeline shifted from October to July to better align the release of IG assessments with the development of the President's Budget as mentioned in OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements.* The previous timing, noted above as concluding in October, limited agency leadership's ability to request

[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021).

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

resources in the next budget year submissions to provide for remediations. The expectation is this change to July will reduce the time between issue identification, resource request, and allocation. For FY 2022, however, OMB granted NASA OIG an extension to submit the FY 2022 IG CyberScope results by September 30, 2022.

FISMA Reporting Metrics

For FY 2022, we used the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, which were developed as a collaborative effort among OMB, DHS, and CIGIE, in consultation with the Federal Chief Information Officer (CIO) and Chief Information Security Officers (CISO). FY 2022 Core IG Metrics represent a continuation of work begun in FY 2016 when the IG metrics were aligned with the five function areas in NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. 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.

Within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and 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 FISMA Reporting Metrics classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security. Table 1 details the five maturity levels to assess an agency's information security program for each Cybersecurity Framework function.

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.

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

The scope of our evaluation was conducted for the period between October 1, 2021, and September 30, 2022. It consisted of testing the 20 Core IG Metrics, as shown in Appendix A, which reflects the results of our assessment of NASA's information security program and practices.

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

Evaluation Results

We determined the maturity level for each function and domain based on our testing of the 20 questions in the FY 2022 Core IG Metrics. Our evaluation was based on a majority of the component scores for each domain and function. The overall maturity level of the information security program was determined as Consistently Implemented (Level 3) and, as such, was not effective for the period October 1, 2021, through September 30, 2022. In addition, more controls need to be implemented in addition to those tested above for NASA to reach Managed and Measurable (Level 4), which is OMB's benchmark for an effective information security program.

NASA's FY 2022 maturity levels for the nine domains and the overall level are presented in Table 2.

Table 2: NASA's FY 2022 Maturity Levels

Function	Maturity Level	
Function 1: Identify		Defined (Level 2)[9]
• Risk Management	Defined (Level 2)	
• Supply Chain Risk Management	Consistently Implemented (Level 3)	
Function 2: Protect		Consistently Implemented (Level 3)
• Configuration Management	Consistently Implemented (Level 3)	
• Identity and Access Management	Consistently Implemented (Level 3)	
• Data Protection and Privacy	Consistently Implemented (Level 3)	
• Security Training	Consistently Implemented (Level 3)	
Function 3: Detect—Information Security Continuous Monitoring		Defined (Level 2)
Function 4: Respond—Incident Response		Consistently Implemented (Level 3)
Function 5: Recover—Contingency Planning		Consistently Implemented (Level 3)
Overall		Consistently Implemented (Level 3)
Overall		**Not Effective**

The Chief Information Officer 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 domain's assessed maturity level and provide the Chief Information Officer with recommendations to remediate deficiencies.

Risk Management: We determined NASA's overall maturity level for the Risk Management program was Defined (Level 2). 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 program and maintains hardware and software, including on-premises, cloud, third-party systems, and system interconnections. RISCS data includes information system authorization to operate (ATO) package, Security Assessment Report (SAR), Business Impact Analysis (BIA), system inventory

[9] The Identify Function maturity level was calculated by the majority maturity level for 6 metrics, 1 Ad Hoc, 3 Defined, and 2 Consistently Implemented. As a result, the maturity level for the Identify Function was Defined.

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

information, and vulnerability management data to track NASA's compliance across the enterprise. RISCS is supplemented by multiple sources and tools to manage the compliance of NASA's information.

Our testing noted that information in RISCS was not current. Specifically, RMA noted:

- Two of the three operational systems selected for testing did not update their ATOs and system-level SARs on a continuous or annual basis;
- One of the three operational systems selected for testing did not perform a BIA;
- Two of the five systems selected for testing were not in operation but were included in RISCS as operational; and
- One of the three operational systems selected for testing could not provide evidence to demonstrate an up-to-date inventory of all software assets and licenses used within its system boundaries.

RMA also noted NASA did not have policies, procedures, and processes for 1) risk framing, 2) risk response, and 3) risk monitoring to manage cybersecurity risks to comply with NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53).

Because of the limitation of inventory recording software, RISCS could not identify and record all the network devices. To compensate for this limitation, NASA implemented a manual process of recording network devices in its NASA Manual Inventory (NMI) system, which was uploaded in RISCS. However, NASA's Information Security Continuous Monitoring (ISCM) Strategy did not include continuous monitoring and performance measures for NMI as required by NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment.*

NASA did not have a 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.

While NASA information system owners are responsible for maintaining the accuracy and completeness of the information in RISCS, there are no centralized Information Technology (IT) Governance procedures or oversight to test for the completeness and accuracy of the comprehensive portfolio information in RISCS or monitor the performance measures specified in the ISCM strategy.

Without accurate and up-to-date information in RISCS, NASA may make decisions based on inaccurate or incomplete data and may not be unable to provide agency-wide oversight for all its information systems. Further, NASA leadership cannot identify trends and anomalies and may make decisions based on erroneous information. Additionally, NASA leadership cannot determine whether NASA complies with its policies and Federal requirements.

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

Recommendations:

RMA recommends the Office of the Chief Information Officer:

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.
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.
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).
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.
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.
6. Develop policies, procedures, and processes to manage the cybersecurity risks of risk framing, risk response, and risk monitoring in accordance with NASA policy.
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.
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.

NASA manages its Plan of Actions and Milestones (POA&M) to address security weaknesses and prioritize remediation efforts. RMA noted NASA had nine overdue POA&M and 11 unapproved Risk-Based Decision (RBD) submissions for two of the three operational systems selected for testing in FY 2022. NASA's ITS-HBK, *STEP 6: Monitor Policy* (ITS-HBK-AASTEP6. v.1.0.0), which requires all POA&Ms be reviewed and/or updated at least annually in RISCS and RBDs must be reviewed at least yearly by the Information System Owner (ISO) and approved by the Approving Official (AO), as part of its continuous monitoring. NASA noted that, due to the reorganization across the enterprise and conversion to NIST SP-800-53, POA&Ms and RBDs were beyond NASA's ability to achieve the completion date. NASA management also stated the process of updating and approving POA&Ms and RBDs involves layers of reviews, which may cause delays in the approval process.

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

POA&Ms and RBDs not updated and approved in a timely manner may impact the overall risk exposure at NASA. As a result, NASA may not accurately measure the Agency risks related to its information security program.

Recommendations:

RMA recommends the Office of the Chief Information Officer:

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.
10. Ensure that the system owners of the systems selected for testing in this evaluation address its past due POA&Ms and unapproved RBDs.
11. Ensure that the system owner of the system selected for testing in this evaluation addresses its unapproved RBD.

Supply Chain Risk Management: We determined NASA's overall maturity level for the Supply Chain Risk Management (SCRM) program was Consistently Implemented (Level 3). SCRM includes exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain. These threats and vulnerabilities potentially compromise the confidentiality, integrity, or availability of an agency's systems and the information they contain. While NASA has made progress in implementing its SCRM processes to be in accordance with NASA's ITS-HBK, *Information & Communications Technology Supply Chain Risk Management (ICT SCRM)* (ITS-HBK-SCRM. 2810.v1.0.0), and NIST SP 800-53, NASA did not provide sufficient evidence of completed supply chain risk review evaluations. The review process needs more time to mature to measure its effectiveness. In addition, NASA needs to include its supply chain risk reviews in its continuous monitoring practices noted in its ISCM Strategy.

Lack of a supplier risk evaluation process leads to an increase in supplier-related risks where adversaries could 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.

Recommendation:

12. RMA recommends the Office of the Chief Information Officer incorporates supplier risk evaluations into its continuous monitoring practices outlined in NASA's ISCM Strategy.

Configuration Management: We determined NASA's overall maturity level for the Configuration Management program was Consistently Implemented (Level 3). NASA consistently implemented, assessed, and maintained secure configuration settings for its information systems through its policies and procedures through NASA's Security Configuration Website. Further, NASA consistently utilized Security Content Automation Protocol (SCAP) validated software to scan all systems on its network for code-based and configuration-based vulnerabilities. NASA

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

incorporated a lesson-learned process into maintaining and updating its configuration specification policies and website. NASA improved in maintaining an up-to-date, complete, accurate, and readily available enterprise-wide view of the security configurations for all information systems connected to the network. NASA also consistently implemented its flaw remediation policies, procedures, and processes to ensure that patches and software updates are identified, prioritized, tested, and installed in a timely manner. In addition, NASA conducted vulnerability scan updates and obtained and stored its patch management reports centrally through RISCS and Information Technology Security - Enterprise Data Warehouse. In order for NASA to reach a higher maturity level, additional controls and processes need to be designed and implemented.

Identity and Access Management: We determined NASA's overall maturity level for the Identity, Credential, and Access Management (ICAM) program was Consistently Implemented (Level 3). NASA managed its ICAM protocols for its employees and contractors. NASA developed an Identification and Authentication policy to require two-factor authentication for non-privileged users by implementing Personal Identity Verification (PIV) cards. NASA also developed an Identification and Authentication policy to require multifactor authentication for privileged users by implementing PIV cards, which defined their process for provisioning, managing, and reviewing privileged accounts. NASA also developed a process for provisioning, managing, and reviewing privileged accounts, including inventorying, and conducting periodic reviews and adjustments for the privileged user accounts and permissions.

Multifactor authentication (MFA) is a security measure that requires two or more proofs of identity to grant you access. MFA typically requires a combination of something the user knows (pin, secret question), physically possesses (e.g., card, token), or inherently possesses (e.g., fingerprint, retina). NASA policies require MFA for local and remote access to its information systems and ensure that the authentication mechanism is Authentication Assurance Level (AAL) 3 compliant using the PIV card. Two-factor authentication using the PIV card is required for local access to non-privileged accounts. For the three centers selected for testing, MFA compliance ranged from 86% to 92%, which is not in compliance with NASA's ITS-HBK, *Identification and Authentication* (ITS-HBK-2810.17-02B), or NIST' SP 800-53. Further, one of three operational systems selected for testing in this evaluation did not institute PIV card authentication or multifactor authentication for its non-privileged user accounts.

According to NASA officials, due to competing priorities, NASA did not employ sufficient resources to fully comply with 'ITS-HBK-2810.17-02B and 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*, to make all information systems compliant with MFA or PIV in lieu of username and password. While NASA has initiated an effort to ensure PIV compliance across the agency, the effort is still in progress. NASA was not fully PIV compliant because all of its information systems (applications) could not be accessed only via PIV or MFA in lieu of a username and password.

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

Recommendations:

RMA recommends the Office of the Chief Information Officer:

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.
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.

Data Protection and Privacy: We determined NASA's overall maturity level for Data Protection and Privacy program was Consistently Implemented (Level 3). 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). Additionally, the NASA Office of the Chief Information Officer 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: PM- Program Management (PM), PT- PII Processing and Transparency (PT), and SR-Supply Chain Risk Management (SR). Without including PM, PT, and SR controls in the ISCM Strategy, NASA cannot monitor or measure the effectiveness of its controls. 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.

Recommendation:

15. RMA recommends the Office of the Chief Information Officer 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.

Security Training: We determined NASA's overall maturity level for the Security Training program was Consistently Implemented (Level 3). NASA has addressed its identified knowledge, skills, and abilities gaps through talent acquisition. NASA completed and submitted a cybersecurity workforce assessment to Congress in December of 2016 to comply with the Federal Cybersecurity Workforce Assessment Act of 2015 requirements. Further, NASA's Cybersecurity & Privacy Division within the OCIO is undergoing a realignment of its workforce and is evaluating its personnel to ensure that skills and abilities are aligned and that its supervisors and civil service

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

employees have the appropriate training and are associated with the appropriate NIST National Initiative for Cybersecurity Education (NICE) roles. NASA has begun the process of developing policies and procedures to assess its cybersecurity workforce's knowledge, skills, and abilities. However, a cybersecurity workforce assessment has not been completed since 2016. A cybersecurity workforce assessment is used by agencies to assess their cybersecurity workforce and develop a strategy to address workforce gaps. Per the FY 2022 Core IG Metrics, assessments should be updated periodically to account for changes in an agency's risk environment and be a key input when updating the agency's awareness and training strategy/plan.

Without periodically updating its cybersecurity workforce assessment, NASA may not be able to identify the knowledge, skills, and abilities gaps and utilize the necessary training or talent acquisition on NASA's key security workforce. As a result, NASA may not accurately measure the risks related to its information security program.

Recommendations:

RMA recommends the Office of the Chief Information Officer:

16. Establish and implement policies and procedures to periodically update its cybersecurity workforce assessment.

Information Security and Continuous Monitoring: We determined NASA's overall maturity level for the ISCM program was Defined (Level 2). NASA developed an ISCM strategy addressing ISCM requirements. NASA's ISCM strategy incorporated Continuous Diagnostics and Mitigation (CDM) technologies designed to enhance continuous monitoring capabilities, establish qualitative and quantitative performance measures, and describe NASA's current performance measurement practices and capabilities. The ISCM strategy, however, was developed in accordance with NIST SP 800-53 revision 4 and not updated in accordance with revision 5. The ISCM strategy establishes the methods for the collection of information and measuring the information against defined metrics. ISCM strategy is routinely reviewed for relevance and is revised as needed to increase visibility into assets and awareness of vulnerabilities. This further enables data-driven control of the security of an organization's information infrastructure and increases organizational resilience.

In addition, 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.

Further, NASA's ISCM strategy utilized CDM tools to gather key system security information allowing for ongoing assessments and monitoring. However, NASA did not consistently perform ongoing authorization and assessment. Specifically, as noted in the Risk Management section above, two of the three operational systems selected for testing did not update their ATOs and system-level SARs and were not discovered in NASA ISCM control activities. See the Risk Management section above for recommendations for delinquent ATOs and SARs.

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

Recommendation:

17. RMA recommends the Office of the Chief Information Officer 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.

Incident Response: We determined NASA's overall maturity level for the Incident Response program was Consistently Implemented (Level 3). NASA consistently implemented its policies, procedures, and processes for incident detection and analysis. NASA established an Incident Response Plan that provided a detailed description of incident handling, defined common threat vectors for classifying incidents and 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), covered NASA's incident detection and analysis and the accompanying NASA Information Security Incident Response Standard Operating 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. In order for NASA to reach a higher maturity level, additional controls and processes need to be designed and implemented.

Contingency Planning: We determined NASA's overall maturity level for the Contingency Planning program was Consistently Implemented (Level 3). NASA defined the processes for conducting system-level BIA and incorporating the results into its strategy. However, one of the three operation systems did not perform the BIA as required by the NASA's ITS-HBK, *Contingency Planning* (ITS-HBK-2810.08-01A).

See the Risk Management section above for recommendations on BIAs.

NASA's Information System Contingency Plan (ISCP) testing for the selected operational systems contained lessons learned, after-action reports, and issues noted. NASA also performed contingency plan testing and exercises.

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 established. They were maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. We found that NASA's information security program and practices were not effective for the period October 1, 2021, through September 30, 2022, and the overall maturity level of NASA's information security program was Consistently Implemented.

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

Objective, Scope, and Methodology

The objective of this evaluation was to evaluate the effectiveness of NASA's information security program and practices for the period October 1, 2021, through September 30, 2022.

NASA's information system infrastructure consists of office networks or applications and several system service providers. RMA assessed NASA against the FY 2022 Core IG Metrics for five selected systems, three of which were operational. Please see Table 3 for the NASA information systems selected.

Table 3: NASA's System Selection

#	System Name	Location	FIPS 199 Categorization
	Internal and External Systems		
1	Consolidated Information Technology Center (CITC) Data Center	Internal	Moderate
2	Hubble Space Telescope – Space Telescope Operations Control Center – Mission Essential Infrastructure (MEI)	Internal	High
3	Digi Smart Sense	External	Moderate
4	Eventbrite*	External	Low
5	Facilities Asset Management System (FAMS)*	External	Low

*Non-operational System

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),[10] requirements set forth by NASA, NIST, OMB, and as outlined in the FY 2022 Core IG 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 2022 Core IG 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 Federal*

[10] CIGIE's *Quality Standards for Inspection and Evaluation* (Blue Book) (December 2020).

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

Information Systems and Organizations: Building Effective Assessment Plans; NIST SP 800-53; FISMA guidance from CIGIE, OMB, DHS, and NASA policies and procedures.

For each FISMA core metric, we indicated whether NASA achieved each maturity level. We determined the maturity level for each of the nine domains and five functions by a simple majority of the component scores of the maturity level of each core metric within the domain and function in accordance with FISMA Reporting Metrics.

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

Criteria

We focused our FISMA evaluation approach on Federal information security guidelines developed by NASA, NIST, and OMB. 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 2022 FISMA Evaluation.

NIST Federal Information Processing Standards (FIPS) Publications and SPs

- 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 SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- 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*
- 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 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-70, Revision 4, *National Checklist Program for IT products-Guidelines for Checklist Users and Developers*
- 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*

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

- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-157, *Guidelines for Derived PIV Credentials*
- 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, *Version 1.1, Secure Software Development Framework (SSDF)*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessment*
  NIST Cybersecurity Framework (CSF) ID.AM-1–4

OMB Policy Directives

- OMB Circular No, A-123, *Management's Responsibility for Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*
- OMB *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*
- 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*
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Memorandum M-17-09, *Management of Federal High-Value Assets*
- OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on the Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*
- OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*

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

- 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-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*

DHS's Cybersecurity & Infrastructure Security Agency

- Binding Operational Directive 18-02, *Securing High Value Assets*
- Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*
- U.S Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 1

NASA Policies

- ITS-HBK-2810.03-02B, *Planning*
- ITS-HBK 2810.04-01A, *Risk Assessment, Vulnerability Scanning, and Expedited Patching*
- ITS-HBK-2810.05-02B, *System and Service Acquisition*
- ITS-HBK-2810.07-02B, *Configuration Management*
- ITS-HBK-2810.08-01A, *Contingency Planning*
- 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. V1.0.0, *Assessment and Authorization Step-2: Select Policy*
- ITS-HBK-AASTEP5. V.1.0.0, *Assessment and Authorization Step 5: Authorize Policy*

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

- 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*

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

Acronyms

AAL	Authentication Assurance Level
AO	Approving Official
ATO	Authorization To Operate
BIA	Business Impact Analysis
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CITC	Consolidated Information Technology Center
CUI	Controlled Unclassified Information
CSF	Cybersecurity Framework
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	U.S. Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name System
EO	Executive Order
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	Information & Communications Technology
ID	Identity Document
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISO	Information System Owner
IT	Information Technology
ITS-HBK	Information Technology Security Handbook
MEI	Mission Essential Infrastructure
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
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law

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

PM	Program Management
POA&M	Plan of Actions and Milestones
PT	PII Processing and Transparency
RBD	Risk-Based Decision
RISCS	Risk Information Security Compliance System
RMA	RMA Associates, LLC
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SP	Special Publication
SR	Supply Chain Risk Management
SSDF	Secure Software Development Framework
STEM	Science, Technology, Engineering, and Mathematics
TIC	Trusted Internet Connection

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

Appendix A – NASA OIG 2022 IG CyberScope Submission

The Appendix A contents labeled "For Official Use Only" on pages 24 through 45 are not being publicly released.

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

Appendix B – Status of Prior Year Recommendations

The following table provides the status of prior FISMA evaluation recommendations as of November 9, 2022.

Table 4: FY 2021 and FY 2020 FISMA Audit Recommendations

Report & Recommendation No.	Recommendations	Status
IG-21-014, Rec. 2	Implement a monitoring and surveillance process over security controls to ensure that all controls nearing their due date for assessment are properly identified, scheduled for assessment, and assessed prior to the due date.	Closed
IG-21-010, Rec. 3	Assign the personnel resources necessary to ensure the agency's security plans for systems that inherit the controls within the agency's new hybrid common controls system are updated and that those hybrid controls are removed from the ACS system security.	Closed
IG-21-010, Rec. 4	Establish a process to ensure that cost estimates are developed and included for all POA&Ms for the ACS system prior to their establishment and approval in RISCS to ensure that costs are properly captured and included in submissions to OMB.	Closed
IG-20-017. Rec. 1	Ensure that the information system oversight process identifies delinquent control risk assessments and initiates timely corrective action to ensure that security controls are reviewed and tested in conformance with federal and agency requirements.	Repeat – Please refer to the FY 2022 Recommendation 1 in the Risk Management section above
IG-20-017, Rec. 4	Update the current training for system owners and system assessment and authorization staff that covers the requirements for maintaining system security plans and supporting plan documentation in RISCS, as well as RISCS's data protection capabilities	Closed
IG-20-017, Rec. 5	Issue clarifying policy guidance to ensure that information security controls for all active NASA information systems that are categorized as "other than satisfied" are properly supported by either a POA&M or Risk-Based Decision document and track exceptions in Agency-wide monitoring tools.	Closed

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

Report & Recommendation No.	Recommendations	Status
IG-20-017, Rec. 7	Issue clarifying policy guidance that the agency's system authorizing officials should ensure that all active information systems operated for the benefit of NASA, either by the agency or other organizations, are covered by an approved contingency plan, when required.	Closed
IG-20-017, Rec. 8	Issue clarifying policy guidance that the agency's system authorizing officials should implement a formal review process to ensure that contingency plans for all applicable active information systems are reviewed on an annual basis to ensure they accurately reflect system requirements, procedures, organizational structure, and policies.	Closed
IG-20-017, Rec. 9	Develop and implement an effective process to ensure that all IT security handbooks and other IT governance documents are reviewed and updated at least annually in accordance with NASA requirements.	Closed

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

Appendix C – Management Response

National Aeronautics and Space Administration

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

December 9, 2022

Reply to Attn of: Office of the Chief Information Officer

TO: 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 2022" (A-22-11-00-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 2022" (A-22-11-00-FMD), dated November 9, 2022.

In the draft report, the OIG makes 17 recommendations addressed to the Chief Information Officer intended to address several control deficiencies.

Specifically, the OIG recommends the following:

Recommendation 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.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system did not update its Authorization to Operate (ATO) and system-level Security Assessment Report (SAR) on a continuous or annual basis. The Office of the Chief Information Officer's (OCIO) ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency Assessment and Authorization (A&A) Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 2: Design and implement the necessary entity-wide oversight, enforcement mechanisms, and controls to ensure all system-level BIAs are accurate and

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

reviewed annually, as well as ensure the information system owners of the systems selected for testing in this evaluation complete a system-level BIA.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not have a Business Impact Analysis (BIA). The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 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).

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not have a BIA. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information systems were not in operation but were included in the Risk Information Security Compliance System (RISCS) as operational. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not provide evidence to demonstrate

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

an up-to-date inventory of all software assets and licenses. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 6: Develop policies, procedures, and processes to manage the cybersecurity risks of risk framing, risk response, and risk monitoring in accordance with NASA policy.

Management's Response: NASA concurs. NASA agrees with the finding. However, due to the ongoing OCIO Transformation to a centralized, enterprise model, NASA's Enterprise Cybersecurity Risk Management (ECRM) group is not yet able to develop policies, procedures, and processes for risk framing, risk response, and risk monitoring. NASA will perform an assessment of its capabilities in this area and will develop a plan to mature the ECRM function to address the intent of this recommendation.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA partially concurs. NASA's Information Security Continuous Monitoring (ISCM) Strategy document is a high-level document that sets the policy for continuous monitoring at NASA, but it is not an appropriate document to specify processes. The NASA Information Technology Security Handbook, "*Step 6: Monitor Policy*" dated January 2022, specifies the processes for continuous monitoring, including the NASA Manual Inventory (NMI) process to document hardware that cannot support automated tools. The RISCS tool provides the template and submission mechanism for Information System Owners (ISOs) to document manual inventory, as described in the RISCS Operations Guide (ROG). NASA will review and update the handbook to more clearly specify the need to validate manual hardware inventory information as part of continuous monitoring.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. NASA concurs with the finding. However, due to the ongoing OCIO Transformation to a centralized, enterprise model, NASA's ECRM group is not yet able to develop a policy and implement the necessary entity-wide oversight to monitor risk through a risk register and a risk profile. NASA will perform an

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

assessment of its capabilities in this area and will develop a plan to mature the ECRM function to address the intent of this recommendation.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not have Plans of Action and Milestones (POA&M) and Risk Based Decisions (RBD) updated and approved in a timely manner. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 10: Ensure that the system owners of the systems selected for testing in this evaluation address its past due POA&Ms and unapproved RBDs.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not have POA&Ms and RBDs updated and approved in a timely manner. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. This consolidated group will work with the Cybersecurity and Privacy Division (CSPD) FISMA team to see that systems selected for FISMA evaluation have addressed/completed POA&Ms and RBDs. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

Estimated Completion Date: November 17, 2023.

Recommendation 11: Ensure that the system owner of the system selected for testing in this evaluation addresses its unapproved RBD.

Management's Response: NASA concurs. NASA agrees with the findings stated in the conditions that the selected information system does not have POA&Ms and RBDs updated and approved in a timely manner. The OCIO's ongoing Transformation to a centralized, enterprise model includes establishing a consolidated Agency A&A Oversight group. This consolidated group will work with the CSPD FISMA team to see that systems selected for FISMA evaluation have addressed/completed POA&Ms and RBDs. In addition, OCIO is developing an executive cybersecurity scorecard, which will include A&A metrics and will further support oversight activities.

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

Estimated Completion Date: November 17, 2023.

Recommendation 12: Incorporates supplier risk evaluations into its continuous monitoring practices outlined in NASA's ISCM Strategy.

Management's Response: NASA concurs. NASA has 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 can review its continuous monitoring guidance and practices to see how supplier risk evaluations may be best included.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. Identity, Credentials and Access Management (ICAM) is actively working multiple efforts to address Personal Identity Verification (PIV) enforcement at NASA. We are currently rolling out Highest Level Credential which requires users to login to Launchpad-protected applications using a PIV card if they have one. Until this effort, users could choose to use username and password even if they have a PIV card. This summer we modified the new identity process to enforce PIV authentication by default. Finally, we have developed tools that Center points of contact will be directed to use to bulk load users into User Based Enforcement. Workplace & Collaboration Services (WCS) Project management is engaging us to develop a plan to move this forward.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

Management's Response: NASA concurs. NASA's efforts to increase adoption of PIV throughout the enterprise are ongoing and OCIO cannot ensure that selected systems will have fully implemented PIV. However, the OCIO FISMA team will ensure that the selected systems have POA&M and RBD posted in RISCS for systems that have not implemented PIV.

Estimated Completion Date: November 17, 2023.

Recommendation 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.

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

Management's Response: NASA concurs. Management will ensure that the security control families Project Management (PM), Personal Identifiable Information (PII) Processing and Transparency (PT), and Supply Chain Risk Management (SR) are updated and defined within the agency's ISCM strategy.

Estimated Completion Date: November 17, 2023.

Recommendation 16: Establish and implement policies and procedures to periodically update its cybersecurity workforce assessment.

Management's Response: NASA non-concurs. Management does not concur with the finding information or recommendation. NASA provided the initial cybersecurity workforce assessment to Congress in December 2016. NASA does not plan to repeat the assessment unless the Office of Personnel Management updates the assessment requirements and methodology to reflect current practices.

Estimated Completion Date: Not applicable.

Recommendation 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.

Management's Response: NASA concurs. NASA concurs with the finding. However, due to the ongoing OCIO Transformation to a centralized, enterprise model, NASA's ECRM group is not yet able to revise its ISCM policies to document and implement lessons learned based on risk events. NASA will perform an assessment of its capabilities in this area and will develop a plan to mature the ECRM function to address the intent of this recommendation.

Estimated Completion Date: November 17, 2023.

We have reviewed the 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 Jeremy Yagle at (757) 864-9622.

JEFFREY SEATON

Digitally signed by JEFFREY SEATON
Date: 2022.12.12 09:09:23 -05'00'

Jeff Seaton