NASA OFFICE OF INSPECTOR GENERAL

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

December 22, 2020

TO: Jeff Seaton, Authorizing Official
Acting Chief Information Officer

Robert L. Binkley, Information System Owner
Deputy Associate Chief Information Officer for Cybersecurity and Privacy

SUBJECT: Final Memorandum, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System* (IG-21-010, A-20-012-01)

The Federal Information Security Modernization Act of 2014 (FISMA) requires that we conduct annual independent evaluations of information security programs and practices at NASA. As part of this year's evaluation of NASA's information security program, we examined an Agency-operated information system known as an Agency Common System (ACS).[1] This memorandum reports the issues and concerns identified during our evaluation of this system for the authorizing official's and system owner's awareness and action. Relatedly, we reported our overall FISMA evaluation results to the Office of Management and Budget (OMB) on October 30, 2020. See Enclosure I for details on our scope and methodology.

Background

In accordance with FISMA, federal agencies are required to implement policies that ensure information security is addressed throughout the life cycle of every agency information system. FISMA requires an annual independent evaluation of federal information security programs and practices, including the evaluation of a subset of individual systems. FISMA's annual reporting requirements seek to ensure information security management is integrated into agency information technology (IT) operations and practices as they relate to agency systems. The National Institute of Standards and Technology (NIST) is

[1] The specific name of the NASA information system tested during this evaluation has been generalized to protect its operational security.

responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST Special Publication (SP) 800-53, Revision 4, provides a catalog of security and privacy controls to help protect organizations from cyber-attack, natural disasters, structural failure, and human error.[2] Three types of security controls for information systems can be employed by an organization:

1. System-specific controls—controls that provide a security capability for a particular information system only;
2. Common controls—controls that provide a security capability for multiple information systems; or
3. Hybrid controls—controls that have both system-specific and common characteristics.

During this evaluation, we examined and tested information security documentation for the information system that is responsible for the administration and management of all Agency information system common controls. Consequently, this information system and the issues identified during our evaluation has the potential to impact Agency information systems that inherit common controls from this system.

Inspector General FISMA Reporting Metrics

To conduct our evaluation, we used NIST standards and the Inspector General (IG) Metrics for FY 2020, which were developed as a collaborative effort among officials from OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the federal Chief Information Officers (CIO) Council. The IG Metrics assess aspects of information security in areas such as risk management, configuration management, identity and access management, security training, and incident response.[3] The IG Metrics identify 85 information security controls from NIST 800-53, Revision 4, to be tested for FY 2020 (see Enclosure II for the complete list).

[2] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (December 2014).

[3] A copy of the FY 2020 IG Metrics is available at https://www.cisa.gov/publication/fy20-fisma-documents (last accessed October 4, 2020).

RESULTS OF REVIEW

As part of our assessment of NASA's overall information security program for FY 2020, we examined the security policies, procedures, practices, and controls for the ACS information system. We chose this system from a universe of more than 450 NASA and contractor systems based on various criteria, including the NASA Center at which the system was located, the system's Federal Information Processing Standards (FIPS) 199 category, and whether the system was NASA- or contractor-operated. The ACS information system is responsible for the administration and management of all Agency common information security controls and impacts all Agency information systems that inherit common controls from this system.[4]

During our review of the ACS system, we found that NASA has not taken corrective action to address a longstanding deficiency regarding controls previously assessed as ineffective. We also found that a software error permitted an unauthorized data change in the Agency's information security database affecting the accuracy of the assessment status of a control. Further, we found that NASA faced delays in its plans to authorize the Agency's new hybrid common controls system, which serves as the central repository for the Agency's hybrid common controls.[5] Lastly, NASA did not develop cost estimates for the remediation of these control deficiencies. As a result, information systems throughout the Agency face unnecessary risks that may threaten the confidentiality, integrity, and availability of NASA's information.

Issue 1: NASA Has Not Addressed a Deficiency in Agency Common System

We identified two Agency common controls classified as "other than satisfied," which means a deficiency exists with those controls.[6] When an assessment identifies a security control deficiency, OMB, NIST, and NASA policies provide two possible methods to address that deficiency: (1) a Plan of Action and Milestones (POA&M) or (2) a Risk-Based Decision document. The first control was correctly reported as "other than satisfied," but system security officials had not taken appropriate action to address the control deficiency. The second control was inaccurately reported in NASA's Risk Information Security Compliance System (RISCS) as "other than satisfied" due to the RISCS software permitting an unauthorized data change.[7]

[4] Inheritance of a control occurs when an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by internal or external entities other than those responsible for the system or application.

[5] The NASA Office of the Chief Information Officer manages Agency-wide common controls that provide a security capability for multiple information systems at NASA's various locations, as well as other Agency-wide common controls that have both system-specific and common characteristics. These latter controls are known as "hybrid common controls."

[6] FISMA requires that federal agencies periodically test and evaluate information system security policies, procedures, and practices with a frequency depending on risk, but no less than annually. Security control assessors classify controls as "other than satisfied" to indicate they were assessed as less than effective.

[7] NASA launched RISCS in 2016 as a centralized Agency toolset to track and report cybersecurity risks. RISCS assigns risk to the appropriate system security plan, aligns NASA's information technology security controls to the NIST Cybersecurity Framework, and reports Agency risk data to federal dashboards.

Plan of Action and Milestones. A POA&M is a corrective action plan that details resources required to accomplish the elements of the plan, milestones in meeting a task, and scheduled completion dates. NIST requires that "a plan of action and milestones is developed and maintained for common controls that have been determined through independent assessments, to be less than effective." NASA policy considers POA&M management to be crucial for identifying the security posture of any given system within the Agency. POA&M reports provide Agency information security officials with information to track and review progress on the status of corrective actions.

Risk-Based Decision document. A Risk-Based Decision document is an analysis supporting the conclusion that a risk can be accepted without corrective action. NASA policy provides that an authorizing official can accept risks by documenting "an explicit statement of understanding of what risk acceptance and authorization to operate implies."

No Action Taken to Address a Control Deficiency

We found that NASA had not assessed the Agency common control entitled SI-04, Information System Monitoring, since April 2015. Moreover, the control was classified in 2015 as "other than satisfied," but system security officials still had not taken appropriate action to address the control deficiency by developing either a POA&M or Risk-Based Decision document.

Based on discussions with system security officials, both the overdue control assessment and the failure to develop either a POA&M or Risk-Based Decision document were the result of an oversight. However, we believe the oversight was caused, in part, by the Agency Office of the Chief Information Officer (OCIO) not prioritizing and allocating the personnel resources needed to address control weaknesses in the ACS system. Since the system has the ability to affect all NASA systems that inherit controls from it, we are concerned that NASA's failure to address the control deficiency could negatively affect the appropriate monitoring of all NASA systems.

RISCS Software Error

During our review of the ACS system, we found that the RISCS software permitted an unauthorized data change to control SA-09, External Information System Services. At the time of our review, the overall control assessment status was reported in RISCS as "other than satisfied" and dated July 2019. However, we found the correct status should have been "satisfied" based on a May 2019 assessment report.

We discussed the data error with an OCIO security official. After researching the conflicting data, the official concluded that a RISCS software error had permitted another user to enter the unauthorized change subsequent to the input of the May 2019 assessment results. The OCIO took steps to resolve and correct this error during our review. Based on our review of supporting documentation of the corrective action, we are not proposing audit recommendations to address this issue.

Recommendations

We recommend that the Information System Owner:

1. Develop a POA&M or Risk-Based Decision document to address the deficiency in control SI-04.

2. Ensure that control SI-04 is assessed as soon as possible and that all ACS system controls are assessed timely in accordance with FISMA requirements.

Issue 2: Delays in Authorizing the Agency Hybrid Common Controls System Weakened the Agency's Overall Cybersecurity Program

NASA has been in the process of creating a new system security plan for hybrid common controls since September 2019. Those controls currently reside in the ACS system along with Agency common controls and operate under that system's Authorization to Operate (ATO).[8] NASA performed an assessment of the hybrid common controls in January 2020 in order to have the new hybrid common controls system ready for review and authorization. The Agency planned to authorize the new system security plan for the hybrid common controls by the end of July 2020. However, as of September 30, 2020, the new system security plan was not fully developed, presented for review to the authorizing official, or authorized to operate. Subsequent to year end, NASA issued an ATO for the Agency's new hybrid common controls system.

Continued delays in accomplishing the work necessary to authorize the hybrid common controls system occurred because the OCIO did not prioritize the work and allocate the necessary personnel resources to meet their intended timetable. Based on discussions with the ACS security control manager, the OCIO assigned only two people on a part-time basis to address several known issues involving the ACS system and to develop the new hybrid common controls system. Consequently, the development and authorization of the new hybrid common controls system fell behind schedule.

In addition to not maintaining a documented system security plan for hybrid common controls that is authorized to operate during the fiscal year, many of the hybrid common controls that were tested as part of the ACS system were assessed as "other than satisfied." A critical part of developing the new hybrid common controls system is to address weaknesses in the Agency's hybrid common controls through the use of POA&Ms or Risk-Based Decision documents. However, until actions are taken to address POA&Ms for those control weaknesses, the confidentiality, integrity, and availability of NASA information resident in NASA information systems is at risk. Because common and hybrid controls are inherited by all NASA applications, control weaknesses within ACS are significant to the overall agency security posture. Even though the Agency's new hybrid common controls system was authorized to operate on November 4, 2020, NASA still needs to update the Agency's security plans for systems that inherit those controls and then remove those controls from the ACS system security plan.

Recommendations

We recommend that the Information System Owner:

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 plan.

[8] Federal information systems are required by law to obtain a signed ATO in order to process government data. Before an ATO is issued, the agency must categorize the system based on its criticality to government operations, determine what security measures must be implemented, and assess the effectiveness of those measures. When an ATO is issued, it means that the authorizing official has assumed responsibility for any system risks.

Issue 3: POA&M Remediation Costs not Considered

We found that NASA did not develop or include cost estimates for remediation of any of the nine POA&Ms we tested. According to a representative from the OCIO, this occurred because, as a general practice, cost estimates are not included for POA&Ms. We take exception with this, as it is contrary to NASA guidance and inconsistent with best practices for administration and management of remediation efforts for known security weaknesses and vulnerabilities associated with information security controls. NASA's guidance states that information system owners should include any costs, including labor costs, of POA&M remediation activities.[9] Specifically, POA&M cost estimates should include the costs of hardware, software, labor, and other related costs associated with POA&M remediation. The failure to accurately account for the costs associated with a POA&M and its remediation impairs the ability of NASA management to effectively administer, prioritize, and allocate the resources necessary to ensure the timely mitigation of the most-critical security weaknesses and vulnerabilities in its information security program. Further, we are concerned that the failure to properly establish and include cost estimates for POA&Ms amounts to a failure to fully consider and account for all costs associated with IT security and compliance, the result of which is an under-reporting of the Agency's IT infrastructure, security, and management standard investments to OMB.[10]

Recommendations

We recommend that the Information System Owner:

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.

5. Ensure that accurate cost estimates associated with the remediation of security weaknesses listed in POA&Ms are prepared and included for all open POA&Ms in the ACS system.

Management's Response and Our Evaluation

We provided a draft of this memorandum to NASA management who concurred with three of our five recommendations and described actions they plan to take. We consider management's comments to those recommendations responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

Management did not concur with Recommendation 2, stating that while NASA policy requires systems to be assessed annually, it only requires controls to be assessed at least once within a three year period. Since management stated control SI-04 is currently being assessed, we consider the recommendation resolved, and it will be closed upon completion and verification of the planned corrective actions.

Further, management partially concurred with Recommendation 3, agreeing to delete and de-allocate the controls in the ACS system that have been determined to be either hybrid or otherwise non-common controls. While it is the individual system owners' responsibility to ensure their system security plans are updated to reflect changes to the Agency's hybrid controls, NASA developed guidance

[9] ITS-HBK-2810.02-08A, *Security Assessment and Authorization: Plan of Action and Milestones (POA&M)* (effective November 2019).

[10] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (July 2020).

and reports to assist NASA information system owners with this transition and will communicate needed actions and implementation responsibilities in the future. We consider management's comments and proposed actions responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed corrective actions.

Management's comments are reproduced in Enclosure III. Technical comments provided by management have been incorporated as appropriate.

Major contributors to this audit and report include Mark Jenson, Financial Management Director; Joseph Shook, Project Manager; James Pearce; and Aleisha Fisher. Matt Ward provided editorial and graphics assistance.

If you have questions or wish to comment on the quality or usefulness of this memorandum, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Paul K. Martin
Inspector General

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

Cody Scott
Chief Cyber Risk Officer

Enclosures—3

Enclosure I: Scope and Methodology

We performed this evaluation from May 2020 through November 2020 in accordance with the Quality Standards for Inspection and Evaluation issued by CIGIE. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

To answer our objective and gain an understanding of the overall information security program, and to assist in reporting the results to OMB, we performed fieldwork remotely for the system maintained at NASA Headquarters. The scope of this evaluation was NASA cybersecurity documentation and practices required by FISMA. In order to review NASA's compliance with FISMA requirements we interviewed OCIO officials and examined and tested the system security plan and its supporting documentation for existence, completeness, and accuracy to determine the adequacy of the Agency's information security efforts.

We reviewed relevant public laws, regulations, and policies to determine the established guidance and best practices. We obtained and reviewed prior audit reports, external reviews, and various other documents related to NASA's overall information security efforts. We reviewed NASA requirements and criteria for FISMA. The documents we reviewed included the following:

Federal Laws, Policy, Standards, and Guidance

Pub. L. No. 113-283, *Federal Information Security Modernization Act of 2014* (December 2014)

Pub. L. No. 107-347, *E-Government Act of 2002* (December 17, 2002)

Executive Order 13800, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017)

OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (July 10, 2020)

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016)

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006)

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004)

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015)

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011)

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (December 2014, includes updates as of January 22, 2015)

NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018)

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012)

NASA Policy, Requirements, and Guidance

NASA Policy Directive 2810.1E, *NASA Information Security Policy* (January 31, 2020)

NASA Procedural Requirements (NPR) 2800.1B, *Managing Information Technology* (March 20, 2009)

NPR 1600.1A, *NASA Security Program Procedural Requirements* (August 12, 2013)

ITS-HBK 2810.02-08A, *Security Authorization and Assessment: Plan for Action and Milestones (POA&M)* (November 2019)

ITS-HBK 2810.02-02E, *Security Assessment and Authorization* (November 1, 2019)

ITS-HBK 2810.02-05A, *Security Assessment and Authorization: External Information Systems* (October 2016)

Assessment of Data Reliability

We relied on computer-generated data as part of performing this evaluation. We assessed the reliability of RISCS data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced it, and (3) interviewing Agency officials knowledgeable about the data. We determined that the data was sufficiently reliable for the purposes of this memorandum.

Review of Internal Controls

Based on the work performed during this analysis, we reviewed internal controls as they relate to NASA's overall information security efforts and identified weaknesses that could potentially affect the confidentiality, integrity, and availability of NASA data, systems, and networks. We discussed the control weaknesses identified in the body of this memorandum. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General and the Government Accountability Office have issued 18 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at https://oig.nasa.gov/audits/auditReports.html and https://www.gao.gov.

NASA Office of Inspector General

Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices (IG-20-021, August 27, 2020)

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019 (IG-20-017, June 25, 2020)

Cybersecurity Management and Oversight at the Jet Propulsion Lab (IG-19-022, June 18, 2019)

Review of NASA's Information Security Program under the Federal Information Security Modernization for Fiscal Year 2018 Evaluation (ML-19-002, March 6, 2019)

Audit of NASA's Information Technology Supply Chain Risk Management Efforts (IG-18-019, May 24, 2018)

Audit of NASA's Security Operations Center (IG-18-020, May 23, 2018)

Final Memorandum, Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation (IG-18-003, November 6, 2017)

Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation (IG-17-002, November 7, 2016)

Report Mandated by the Cybersecurity Act of 2015 (IG-16-026, July 27, 2016)

Final Memorandum, Review of NASA's Information Security Program (IG-16-016, April 14, 2016)

Government Accountability Office

Priority Open Recommendations: National Aeronautics and Space Administration (GAO-20-526PR, April 23, 2020)

Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation (GAO-19-131, April 29, 2019)

Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93, August 2, 2018)

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation Policies and Practices (GAO-17-549, September 28, 2017)

Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges (GAO-17-533T, April 4, 2017)

Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems (GAO-17-518T, March 29, 2017)

Federal Information Security: Actions Needed to Address Challenges (GAO-16-885T, September 19, 2016)

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems (GAO-16-501, May 18, 2016)

Enclosure II: Information Security Controls Tested

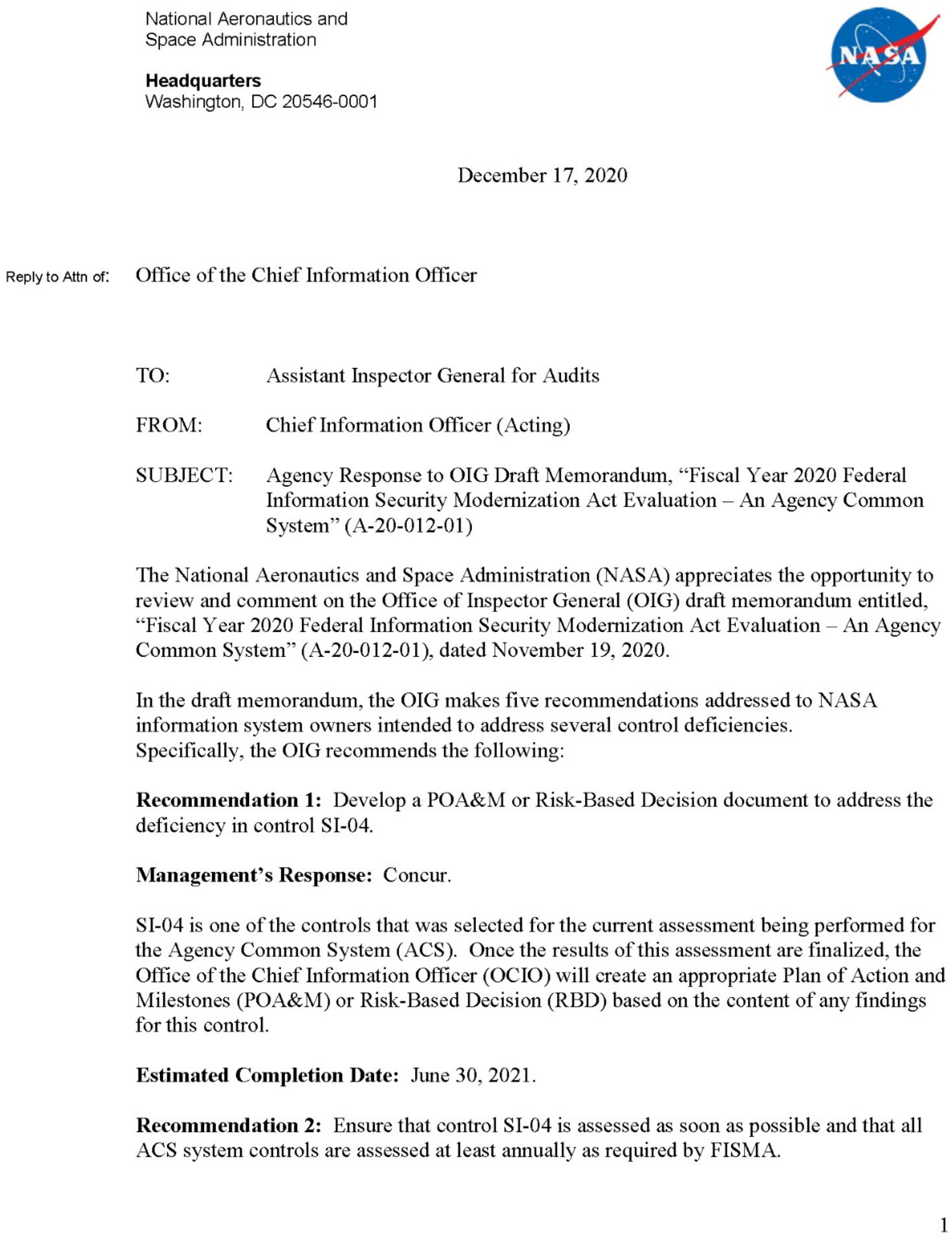
Table 1: NIST SP800-53, Revision 4, Security Controls Tested

#	Information Security Control	FIPS 199 Security Category		
		Low	Moderate	High
1	AC-01 – Access Control Policy and Procedures	X	X	X
2	AC-02 – Account Management	X	X	X
3	AC-05 – Separation of Duties		X	X
4	AC-06 – Least Privilege		X	X
5	AC-08 – System Use Notification	X	X	X
6	AC-11 – Session Lock		X	X
7	AC-12 – Session Termination		X	X
8	AC-17 – Remote Access	X	X	X
9	AC-19 – Access Control for Mobile Devices	X	X	X
10	AT-01 – Security Awareness and Training Policy and Procedures	X	X	X
11	AT-02 – Security Awareness Training	X	X	X
12	AT-03 – Role Based Security Training	X	X	X
13	AT-04 – Security Training Records	X	X	X
14	AU-02 – Audit Events	X	X	X
15	AU-03 – Content of Audit Records	X	X	X
16	AU-06 – Audit Review, Analysis, and Reporting	X	X	X
17	CA-01 – Security Assessment and Authorization Policy and Procedures	X	X	X
18	CA-02 – Security Assessments	X	X	X
19	CA-03 – System Interconnections	X	X	X
20	CA-05 – Plan of Action and Milestones	X	X	X
21	CA-06 – Security Authorization	X	X	X
22	CA-07 – Continuous Monitoring	X	X	X
23	CM-01 – Configuration Management Policy and Procedures	X	X	X
24	CM-02 – Baseline Configuration	X	X	X
25	CM-03 – Configuration Change Control		X	X
26	CM-04 – Security Impact Analysis	X	X	X
27	CM-06 – Configuration Settings	X	X	X
28	CM-07 – Least Functionality	X	X	X
29	CM-08 – Information System Component Inventory	X	X	X
30	CM-09 – Configuration Management Plan		X	X
31	CM-10 – Software Usage Restrictions	X	X	X
32	CP-01 – Contingency Planning Policy and Procedures	X	X	X
33	CP-02 – Contingency Plan	X	X	X
34	CP-03 – Contingency Training	X	X	X
35	CP-04 – Contingency Plan Testing	X	X	X
36	CP-06 – Alternate Storage Site		X	X
37	CP-07 – Alternate Processing Site		X	X
38	CP-08 – Telecommunications Services		X	X
39	CP-09 – Information System Backup	X	X	X
40	IA-01 – Identification and Authentication Policy and Procedures	X	X	X
41	IA-02 – Identification and Authentication (Organizational Users)	X	X	X
42	IA-05 – Authenticator Management	X	X	X
43	IA-07 – Cryptographic Model Authentication	X	X	X

#	Information Security Control	FIPS 199 Security Category		
		Low	Moderate	High
44	IA-08 – Identification and Authentication (Non-Organizational Users)	X	X	X
45	IR-01 – Incident Response Policy and Procedures	X	X	X
46	IR-04 – Incident Handling	X	X	X
47	IR-06 – Incident Reporting	X	X	X
48	IR-07 – Incident Response Assistance	X	X	X
49	MP-03 – Media Marking		X	X
50	MP-06 – Media Sanitization	X	X	X
51	PL-02 – System Security Plan	X	X	X
52	PL-04 – Rules of Behavior	X	X	X
53	PL-08 – Information Security Architecture		X	X
54	PS-01 – Personnel Security Policy and Procedures	X	X	X
55	PS-02 – Position Risk Designation	X	X	X
56	PS-03 – Personnel Screening	X	X	X
57	PS-06 – Access Agreements	X	X	X
58	PM-05 – Information Inventory	Independent of any system impact level		
59	PM-07 – Enterprise Architecture			
60	PM-08 – Critical Infrastructure Plan			
61	PM-09 – Risk Management Strategy			
62	PM-11 – Mission/Business Process Definition			
63	RA-01 – Risk Assessment Policy and Procedures	X	X	X
64	RA-02 – Security Categorization	X	X	X
65	RA-05 – Vulnerability Scanning	X	X	X
66	AR-04 – Privacy Monitoring and Auditing (Appendix J)	X	X	X
67	AR-05 – Privacy Awareness and Training (Appendix J)	Independent of any system impact level		
68	SA-03 – System Development Life Cycle			
69	SA-04 – Acquisition Process	X	X	X
70	SA-08 – Security Engineering Principles		X	X
71	SA-09 – External Information System Services	X	X	X
72	SA-12 – Supply Chain Protection			X
73	SC-07 (10) – Boundary Protection | Prevent Unauthorized Exfiltration			
74	SC-08 – Transmission Confidentiality and Integrity		X	X
75	SC-10 – Network Disconnect		X	X
76	SC-13 – Cryptographic Protection	X	X	X
77	SC-18 – Mobile Code		X	X
78	SC-28 – Protection of Information at Rest		X	X
79	SI-02 – Flaw Remediation	X	X	X
80	SI-03 – Malicious Code Protection	X	X	X
81	SI-04 – Information System Monitoring	X	X	X
82	SI-04 (4) – Information System Monitoring | Inbound and Outbound Communications Traffic		X	X
83	SI-04 (18) – Information System Monitoring | Analyze Traffic / Covert Exfiltration			
84	SI-07 (8) – Software, Firmware, and Information Integrity | Auditing Capability for Significant Events			
85	SE-02 – Privacy Incident Response (Appendix J)	Independent of any system impact level		

Source: NIST SP 800-53, Revision 4, Appendixes D and J

Enclosure III: Management's Comments



National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

December 17, 2020

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer (Acting)

SUBJECT: Agency Response to OIG Draft Memorandum, "Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System" (A-20-012-01)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft memorandum entitled, "Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System" (A-20-012-01), dated November 19, 2020.

In the draft memorandum, the OIG makes five recommendations addressed to NASA information system owners intended to address several control deficiencies.
Specifically, the OIG recommends the following:

Recommendation 1: Develop a POA&M or Risk-Based Decision document to address the deficiency in control SI-04.

Management's Response: Concur.

SI-04 is one of the controls that was selected for the current assessment being performed for the Agency Common System (ACS). Once the results of this assessment are finalized, the Office of the Chief Information Officer (OCIO) will create an appropriate Plan of Action and Milestones (POA&M) or Risk-Based Decision (RBD) based on the content of any findings for this control.

Estimated Completion Date: June 30, 2021.

Recommendation 2: Ensure that control SI-04 is assessed as soon as possible and that all ACS system controls are assessed at least annually as required by FISMA.

Management's Response: Non-concur.

SI-04 is being assessed in the current assessment of the ACS. However, while an information system must be assessed annually, there is no requirement that every control must be assessed annually; per ITS-HBK-2810.02-04A, Continuous Monitoring – Security Control Ongoing Assessment and Authorization, assessments are conducted annually, and all controls must be assessed at least once within a three-year period.

Estimated Completion Date: N/A.

Recommendation 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.

Management's Response: Partially-concur.

OCIO agrees with the intent of this recommendation and is working to ensure that all NASA authorization packages that should inherit controls from the Agency's new hybrid common controls will be able to do so as seamlessly as possible. OCIO is working with the Risk Information Security Compliance System (RISCS) team to delete and de-allocate the controls in the ACS that have been determined to be either hybrid or otherwise non-common controls. The RISCS team has also developed guidance and reports to assist all NASA Information System Owners (ISOs) with this transition and will communicate needed actions and ISO responsibilities to implement through coordinated outreach.

We believe this described approach meets the recommendation's intent, since NPR 2810.1 "Security of Information Technology" stipulates that the primary funding organization of the information system and associated ISO have management responsibility for maintaining their individual System Security Plans (SSP) and planning for adequate support resources. To fully achieve this recommendation, ISOs for systems that inherit the Agency's hybrid controls are responsible for ensuring: a) that they have sufficient resources to maintain controls generally, and b) that their SSP is updated and assessed to reflect changes to the hybrid controls.

Estimated Completion Date: February 28, 2022.

Recommendation 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.

Management's Response: Concur.

OCIO will update the appropriate Assessment and Authorization handbooks to provide guidance for how POA&M cost estimates should be developed and included for all POA&Ms (which will include POA&Ms for the ACS).

Estimated Completion Date: March 31, 2022.

Recommendation 5: Ensure that accurate cost estimates associated with the remediation of security weaknesses listed in POA&Ms are prepared and included for all open POA&Ms in the ACS system.

Management's Response: Concur.

OCIO concurs with this recommendation; however, since there currently is not a NASA methodology or guidance for establishing POA&M cost estimates (see Recommendation 4), this will be completed and accurate to the best of our current ability and knowledge.

Estimated Completion Date: April 30, 2021.

We have reviewed the draft report for information that should not be publicly released and concluded the report contains no such information.

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 Fatima Johnson on (202) 358-1631.

JEFFREY SEATON Digitally signed by JEFFREY SEATON
Date: 2020.12.17 16:31:31 -05'00'

Jeff Seaton