NASA OFFICE OF INSPECTOR GENERAL

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

February 16, 2021

TO: Angela M. Nolen, Authorizing Official
Manager, Resource Management Office, Marshall Space Flight Center

Todd M. Freestone, Information System Owner
Radio Frequency Communications Engineer, Marshall Space Flight Center

SUBJECT: Final Memorandum, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Communications System* (IG-21-013, A-20-012-04)

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, we examined an Agency-operated information system known as a Center Communications System (CCS), operated at the Marshall Space Flight Center (Marshall).[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 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

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

disasters, structural failure, and human error.[2] NIST also published a set of procedures for conducting assessments of security and privacy controls employed within federal information systems and organizations.[3]

Federal and NASA policies provide two possible methods to address information security control deficiencies that result from control assessments: (1) Plan of Action and Milestones (POA&M) or (2) Risk-Based Decision document (RBD).

Plan of Action and Milestones (POA&M). 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. These plans serve as NASA's primary management tool to remediate information security-related weaknesses and are maintained in the Risk Information Security Compliance System (RISCS) database.[4] POA&M reports provide Agency information security officials with information to track and review progress on corrective actions. These reports also provide a basis for an authorizing official to approve or revoke an information system's authority to operate. NASA policy considers POA&M management to be crucial for identifying the security posture of any given system within the Agency.

Risk-Based Decision document (RBD). An RBD 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."

During this evaluation, we examined and tested information security documentation for the information system that controls global positioning system (GPS) simulators, collects GPS test data, and supports radio frequency communication tests and activities.

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.[5] 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* (April 2013).

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

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

[5] 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 CCS system. The CCS system is responsible for controlling simulators and collecting test data performed in support of various communication tests and activities. 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.

During our review of the CCS system, we found that NASA had not taken corrective action to address information security control deficiencies in a timely manner. Specifically, we found that NASA failed to prepare POA&Ms or RBDs for information security controls that were deemed ineffective during recent security assessments, which are performed periodically by NASA as part of its continuous monitoring process. As a result, information security controls for the CCS system face unnecessary risks that—until the ineffective controls have been properly mitigated—may threaten the confidentiality, integrity, and availability of information that is processed, stored, or transmitted by the CCS system.

Information Security Control Deficiencies Have Not Been Addressed in a Timely Manner

We performed our review of the most current CCS system security plan, which was dated May 10, 2019. We found NASA did not prepare POA&Ms or RBDs for 11 of the controls it assessed as "other than satisfied."[6] Federal and NASA policies require either a POA&M or RBD be prepared when an assessment identifies a security control deficiency resulting in an "other than satisfied" classification.

In September 2020, the CCS system owner stated the system controls were in the process of being reassessed and the security documentation would be updated in RISCS, the Agency's information security management tool. We examined the updated assessment documentation as of September 29, 2020, and noted that 6 of the 11 controls we originally identified as not supported by a POA&M or RBD had been reassessed by the Agency as "satisfied" or effective, thus not requiring those documents. Additionally, during our review the Agency prepared RBDs to demonstrate risk acceptance for 4 of the 11 controls deemed "other than satisfied" in the earlier assessment. However, as of December 4, 2020, those RBDs had not been reviewed or approved by the Information System Security Officer. Consequently, we still consider those four controls deficient and lacking an approved RBD. Finally, we noted that 1 of the 11 controls lacking a POA&M or RBD—CM-08, Information System Component Inventory—was not reassessed during NASA's 2020 security assessment.[7] While that control is scheduled to be assessed in 2021, it is still categorized as "other than satisfied" and is not covered by a POA&M to remediate the deficiency or an RBD to accept the risk without corrective action.

[6] FISMA requires that federal agencies periodically test and evaluate information system security policies, procedures, and practices with a frequency depending on risk, but not less than annually. Security control assessors at NASA classify controls as "other than satisfied" to indicate they were assessed as less than effective.

[7] The control CM-08, Information System Component Inventory, requires organizations to develop and document an inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary of the information system, and is granular enough for tracking and reporting.

Recommendations

We recommend that the Information System Owner:

1. Work with the Information System Security Officer to ensure the timely review and approval of the RBDs submitted in September 2020.

2. Ensure that control CM-08, Information System Component Inventory, is assessed as soon as possible and that all CCS system controls are assessed timely in accordance with FISMA requirements.

Management's Response and Our Evaluation

We provided a draft of this memorandum to NASA management who concurred with both of our recommendations and described actions they plan to take. We consider management's comments to our recommendations responsive; therefore, the recommendations are 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; Aleisha Fisher; and James Pearce. 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—2

Enclosure I: Scope and Methodology

We performed this evaluation from May 2020 through January 2021 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 Marshal Space Flight Center. 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* (April 2013, 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 of Action and Milestones (POA&M)* (November 2019)

ITS-HBK 2810.02-02E, *Security Assessment and Authorization* (November 6, 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 evaluation.

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 address those identified weaknesses.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General and the Government Accountability Office have issued 19 reports of significant relevance to the subject of this report. Reports can be accessed at https://oig.nasa.gov/audits/auditReports.html and https://www.gao.gov.

NASA Office of Inspector General

Final Memorandum, Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System (IG-21-010, December 22, 2020)

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 Laboratory (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 28, 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

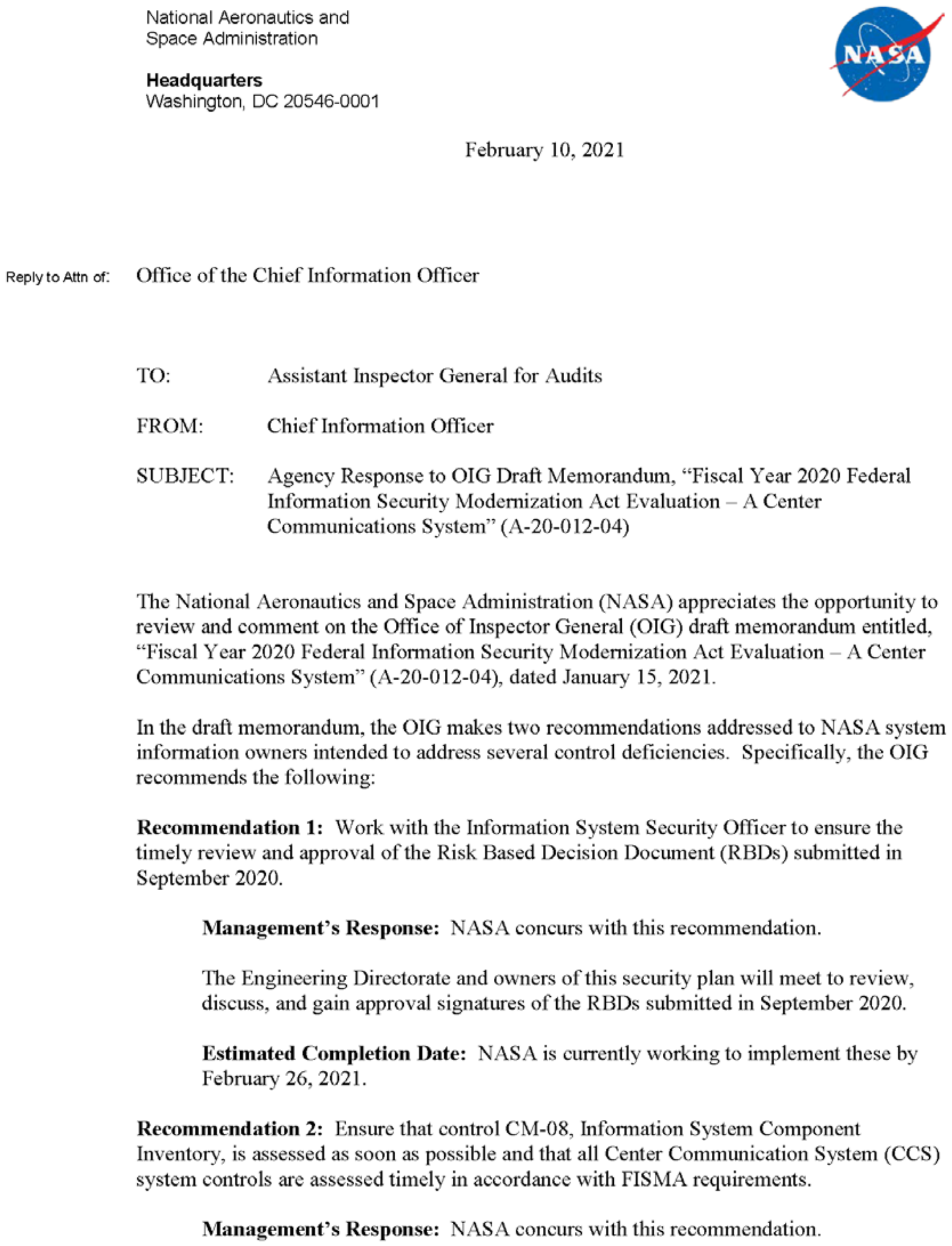
Table 1: NIST SP 800-53, Revision 4, Security Controls Tested

#	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)	Independent of any system impact level		
67	AR-05 – Privacy Awareness and Training (Appendix J)			
68	SA-03 – System Development Life Cycle	X	X	X
69	SA-04 – Acquisition Process	X	X	X
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

February 10, 2021

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 Memorandum, "Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Communications System" (A-20-012-04)

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 – A Center Communications System" (A-20-012-04), dated January 15, 2021.

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

Recommendation 1: Work with the Information System Security Officer to ensure the timely review and approval of the Risk Based Decision Document (RBDs) submitted in September 2020.

Management's Response: NASA concurs with this recommendation.

The Engineering Directorate and owners of this security plan will meet to review, discuss, and gain approval signatures of the RBDs submitted in September 2020.

Estimated Completion Date: NASA is currently working to implement these by February 26, 2021.

Recommendation 2: Ensure that control CM-08, Information System Component Inventory, is assessed as soon as possible and that all Center Communication System (CCS) system controls are assessed timely in accordance with FISMA requirements.

Management's Response: NASA concurs with this recommendation.

The Engineering Directorate and owners of this security plan will meet to assess the Information System Component Inventory as submitted in the security plan.

Estimated Completion Date: NASA is currently working to implement these by February 26, 2021.

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 Fatima Johnson on (202) 358-1631.

JEFFREY SEATON Digitally signed by JEFFREY SEATON
Date: 2021.02.10 18:14:50 -05'00'

Jeff Seaton
Chief Information Officer