NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

March 2, 2021

TO: Michael J. Bolger, Authorizing Official
Program Manager, Kennedy Space Center

Jerrace C. Mack, Information System Owner
Information System Security Officer, Kennedy Space Center

Robert G. Van Arsdalen, Information System Owner
Cybersecurity Technical Lead, Kennedy Space Center

SUBJECT: Final Memorandum, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Command and Control System* (IG-21-014, A-20-012-02)

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 Command and Control System (CCCS), located at Kennedy Space Center (Kennedy).[1] This memorandum reports the issues identified during our evaluation of this system for the authorizing official's and system owners' awareness and action. Relatedly, on October 30, 2020, we reported our overall FISMA evaluation results to the Office of Management and Budget (OMB). 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

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

a catalog of security and privacy controls to help protect organizations from cyber-attack, natural disasters, structural failure, and human error.[2] NIST also published a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations.[3] FISMA requires that federal agencies periodically test and evaluate information system security policies, procedures, and practices with a frequency based on risk, but not less than annually.

Information Security Control Assessments. Control assessments determine the extent to which information security controls are implemented correctly, operate as intended, and produce the desired outcomes in meeting security requirements. According to NIST, the FISMA requirement for annual assessments can be met using the results of continuous monitoring.[4] NASA employs independent security control assessors to conduct security assessments of NASA information systems as required by NIST; at Kennedy, control assessors are part of the Center's IT Security Office and are organizationally independent of the CCCS system.

During this evaluation, we examined and tested information security documentation for the information system that operates, monitors, and coordinates ground equipment and facilitates communications among NASA personnel at Kennedy and other NASA facilities.

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] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, defines continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. NIST provides that organizations establish the frequency for ongoing security control assessments in accordance with continuous monitoring strategies.

[5] A copy of the FY 2020 IG Metrics is available at https://www.cisa.gov/publication/fy20-fisma-documents (last accessed December 2, 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 CCCS 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.

During our review of the CCCS system, we found that approximately 11 percent of the security controls we reviewed were overdue for independent assessment. As a result, NASA lacks assurance that system security controls are implemented correctly, operating as intended, and are producing the desired security outcomes.

Issue: Independent Security Control Assessments Were Not Performed

During our review of the CCCS system, we identified a significant number of overdue control assessments. Specifically, we found that 9 of the 85 information security controls we reviewed (almost 11 percent) had not been independently assessed in more than 3 years.[6] Further, one of those 9 security controls had not been assessed in more than 5 years.

Federal and Agency Requirements for Control Assessments

FISMA requires that federal agencies periodically test and evaluate information system security controls with a frequency based on risk, but not less than annually. Since the CCCS system is subject to continuous monitoring, the 9 controls we identified as having overdue control assessments did not require an annual independent assessment. However, Kennedy policy requires an independent assessment of controls not less than once every 3 years. In November 2019, the Center's Engineering Directorate issued a standard operating policy and practice (SOPP) document to define the security assessment and authorization requirements specifically applicable to the CCCS system.[7] The SOPP provides that the CCCS system security assessment and authorization process must be completed every 3 years or when there is a change that affects the system's security posture.

A Process Failure and Lack of Due Diligence Led to Overdue Control Assessments

Overdue control assessments associated with the Kennedy system that we reviewed were the result of the IT Security Office failing to follow established procedures for conducting and documenting assessments and a lack of due diligence by the system owners. We discussed the overdue control assessments with system owners, other system IT security officials, and a lead control assessor from the IT Security Office.[8] They acknowledged there is no evidence that the 9 overdue assessments had been

---

[6] We measured the timeliness of independent control assessments as of June 29, 2020. On that date, we obtained a copy of the System Security Plan, which we used as the basis for our review.

[7] KSC-NE-SCCS-ITS-SOPP-50004, Revision F, *Standard Operating Policies & Practices (SOPP) for Security Assessment and Authorization* (November 11, 2019).

[8] The security control assessor who was responsible for CCCS system during the period covered by our review is no longer a NASA employee.

performed. However, they speculated that the security control assessor may have performed individual control assessments as part of an overall system review conducted in February 2020, but failed to record the individual assessments in NASA's Risk Information Security Compliance System (RISCS).[9] We note that even if the 9 control assessments were performed in February 2020, those controls still had not been independently assessed in more than 3 years. Based on our discussions, we concluded that the overdue control assessments were primarily caused by a failure of process in the IT Security Office.

The overdue control assessments also resulted from a lack of due diligence by system owners. The prevalence of overdue assessments indicated that system owners did not have an effective process in place to identify controls nearing the due date for independent assessment and then coordinate with the IT Security Office to ensure that the control assessments were performed in a timely manner.

Consequently, as a result of the CCCS system's overdue control assessments, NASA currently lacks the assurance that CCCS system controls are implemented correctly, operate as intended, and produce the desired security outcomes. Further, without the assurance that security controls are functioning properly and as intended, the Agency faces unnecessary risks that could threaten the confidentiality, integrity, and availability of NASA's information, contained, stored, or processed within the CCCS system.

Recommendations

We recommend that the Information System Owners:

1. Ensure that all overdue control assessments are performed by an independent security control assessor from the Kennedy IT Security Office.

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.

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.

[9] 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.

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–3

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 Kennedy Space 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 IT 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 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 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
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 25, 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 Command and Control System" (A-20-012-02)

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 Command and Control System" (A-20-012-02), dated January 26, 2021.

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

Recommendation 1: Ensure that all overdue control assessments are performed by an independent security control assessor from the KSC IT Security Office.

Management's Response: Concur. A new independent assessment is scheduled for February and will be completed before March 1, 2021. In order to mitigate future concerns, we are starting in February 2021, a meeting series for a monthly tag-up between the Exploration Ground Systems (EGS) Information Technology (IT) Security team and KSC IT Security Team representatives to ensure better communications of expectations associated with EGS IT Security plan submissions. EGS IT Security will add appropriate program milestones to the schedule to ensure assessments align with program need dates. EGS IT Security will coordinate with the KSC IT Security Office as required to ensure partnership.

Estimated Completion Date: March 31, 2021.

Recommendation 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.

Management's Response: Concur. The KSC IT Security Team and EGS Information Security Officer (ISO) will partner a list of controls to be assessed in the upcoming annual review (part of current process). EGS is requesting that the annual review include controls with due dates within the upcoming 18 months (KSC Security Office default is 12 months, unless customer requests otherwise). An 18-month window will provide EGS and the KSC IT Security Office with some flexibility to ensure control assessment due dates are not missed. In addition, after the Authorizing Official (AO) panel briefing, the NASA Engineering (NE) IT Security will execute a Risk Information Security Compliance System (RISCS) report to ensure no controls show past due.

Estimated Completion Date: August 31, 2022.

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: 2021.02.26 13:41:59 -05'00'

Jeff Seaton
Chief Information Officer