NASA
National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

EVALUATION OF NASA'S INFORMATION SECURITY PROGRAM UNDER THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2019

June 25, 2020

Report No. IG-20-017

Office of Inspector General

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit https://oig.nasa.gov/hotline.html. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, D.C. 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas or request future audits, contact the Assistant Inspector General for Audits at https://oig.nasa.gov/aboutAll.html.

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019

June 25, 2020 IG-20-017 (A-19-011-00)

WHY WE PERFORMED THIS EVALUATION

In fiscal year (FY) 2019, NASA spent approximately $2.3 billion on computer systems, networks, and information technology (IT) services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure among other things. Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that provides information security protections commensurate with the risks and magnitude of harm that could result from unauthorized access, disclosure, modification, or destruction of agency information. NASA's information security program is managed through the Risk Information Compliance System (RISCS), a data repository that identifies and maintains an inventory of the Agency's hardware and software, including a system security plan (SSP) and a contingency plan for each information system. To determine the effectiveness of an agency's information security program, FISMA requires each agency's Inspector General or an independent external auditor to conduct an annual independent evaluation using the FY 2019 IG FISMA Reporting Metrics and report the results to the Office of Management and Budget (OMB).

In October 2019, we reported to OMB that for FY 2019 NASA's information security program was rated at Level 2, "Defined," out of five levels, with Level 5, "Optimized," being the most effective. This evaluation further examines NASA's information security program based on the FISMA guidance by examining SSPs, contingency plans, and IT security handbooks and other governing documents. To complete this effort, we performed fieldwork at four Centers; reviewed six information systems; interviewed Agency officials, information systems owners, and information security officers; and reviewed relevant public laws, regulations, and policies.

WHAT WE FOUND

NASA has not implemented an effective Agency-wide information security program. SSP documentation for all six information systems we reviewed contained numerous instances of incomplete, inaccurate, or missing information. We also performed a limited review of the Agency Common Control (ACC) system, which aggregates and manages common controls across all Agency information systems, and found that many controls were classified as "other than satisfied," indicating they had been assessed as less than effective. Moreover, the NASA Office of the Chief Information Officer (OCIO) has not addressed these deficiencies in the ACC SSP. At NASA, Chief Information Security Officers (CISO) located at each Center are responsible for providing oversight to ensure that accurate records on the Agency's information systems, including SSPs, are documented in RISCS. However, these weaknesses in SSPs occurred because Center CISO's often are responsible for managing large portfolios of information systems and do not always have resources available to ensure data in RISCS for each system are accurate and complete. The issues we identified during this review occurred primarily because the OCIO does not consistently require the use of RISCS as the Agency's information security management tool. Further, NASA information security personnel are not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that delinquent information security assessments are identified and mitigated. As a result, information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA's information.

Of the six information systems reviewed, we found that four were operating without current contingency plans. While three of the four systems eventually updated their contingency plans in RISCS during the course of our evaluation, these systems had been operating under outdated plans for as long as 4 years. The fourth system is currently operating under a 2016 contingency plan. NASA policy requires information system owners to review contingency plans for accuracy and completeness at least annually or more frequently if significant changes occur to any element of the plan. The Agency authorizing officials responsible for reviewing and approving information systems, including contingency plans, are not performing regularly scheduled testing to determine whether the information in RISCS is accurate, up-to-date, and usable by senior IT leadership. Moreover, the number of systems without a current or available contingency plan in RISCS puts NASA at an unnecessarily high risk by hindering the Agency's ability to recover information systems if needed in an effective and efficient manner, thus threatening the confidentiality, integrity, and availability of NASA information maintained in those systems.

During our review of selected OCIO IT security handbooks and other related governance documents, we found that 27 of 45 documents had not been reviewed and approved in more than 1 year and 8 that not been reviewed in over 3 years. OCIO policy states that IT security handbooks shall be reviewed or updated on an annual basis or more frequently if appropriate. However, the OCIO policy management process does not provide adequate oversight of this process or a reliable list of policies requiring review. OCIO officials stated that they intend to change the review process in FY 2020 but expressed concern about the sufficiency of resources to complete this task. Failure to update NASA policy and procedures in a timely manner increases the risk that Agency personnel will employ out-of-date information security practices. The timely review and update of IT governance documents is a basic internal control necessary for the effective and efficient operation of Agency information systems.

What We Recommended

In order to strengthen the Agency's information security program, we made nine recommendations to the Acting Chief Information Officer to include: (1) ensuring the information system oversight process identifies delinquent control risk assessments and timely corrective action initiated to ensure that controls are reviewed and tested; (2) issuing clarifying policy guidance to ensure that controls for all active NASA information systems that are categorized as "other than satisfied" are properly supported; (3) issuing clarifying policy guidance that the Agency's system authorizing officials should ensure that all active information systems operated for the benefit of NASA are covered by an approved contingency plan, when required; (4) issuing clarifying policy guidance that the Agency's system authorizing officials should implement a review process to ensure that contingency plans for all applicable active information systems are reviewed on an annual basis; and (5) developing and implementing 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.

We provided a draft of this report to NASA management, who concurred with our recommendations and described planned actions to address them. We consider management's comments responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

For more information on the NASA Office of Inspector General and to view this and other reports visit https://oig.nasa.gov/.

TABLE OF CONTENTS

Acronyms

ACC	Agency Common Control
CIO	Chief Information Officer
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	fiscal year
IG	Inspector General
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RISCS	Risk Information Security Compliance System
SP	Special Publication
SSP	system security plan

INTRODUCTION

In fiscal year (FY) 2019, NASA spent approximately $2.3 billion on computer systems, networks, and information technology (IT) services used to, among other things, control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure. These IT assets range from mobile devices and laptops to small unmanned aircraft systems to the NASA Center for Climate Simulation that utilizes a supercomputer capable of performing nearly 160 trillion operations per second. Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals. However, NASA has struggled to implement an effective IT security and governance infrastructure, and the issue has been a long-standing top management and performance challenge for the Agency.[1]

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that provides information security protections commensurate with the risks and magnitude of harm that could result from unauthorized access, disclosure, modification, or destruction of Agency information. To determine the effectiveness of this program, FISMA requires each agency's Inspector General (IG) or an independent external auditor to conduct an annual independent evaluation using the FY 2019 IG FISMA Reporting Metrics (IG Metrics) and report the results to the Office of Management and Budget (OMB).

In October 2019, we reported to OMB that for FY 2019 NASA's information security program was rated at Level 2 out of five levels, with Level 5 being the most effective. This evaluation further examines NASA's information security program based on FISMA guidance. Specifically, we assessed the effectiveness of the Agency's system security plans, contingency plans, and IT security handbooks and other governing documents. See Appendix A for details on the evaluation's 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. Federal agencies are also required to develop agency-wide security awareness training to inform personnel, including contractors and other users of their information systems, of the need to comply with agency policies designed to reduce information security risks. Additionally, FISMA requires an annual independent evaluation of a federal agency's information security program and practices in order to determine and assess its effectiveness. The annual reporting requirements imposed by FISMA seek to help ensure information security management is integrated into agency IT operations and practices. To assist in annual FISMA testing, IG Metrics based on standards developed by the National Institute of Standards and Technology (NIST) are used by Offices of Inspector General (OIG) and oversight entities. NIST is responsible for developing information security standards and guidelines, including minimum

[1] We first identified IT security and governance as a top management and performance challenge in 2011, and have included on every annual report since, including our most recent report. NASA Office of Inspector General, *2019 Report on NASA's Top Management and Performance* Challenges (November 13, 2019).

requirements for federal information systems. To help protect organizational operations, assets, and individuals from a diverse set of threats, including hostile cyber-attacks, natural disasters, structural failures, and human errors, NIST produced a special publication—NIST Special Publication (SP) 800-53, Revision 4—to provide a catalog of security and privacy controls for federal information systems and organizations.[2]

Inspector General FISMA Reporting Metrics

Based on NIST standards, the IG Metrics for FY 2019 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, in consultation with the Federal Chief Information Officer 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 metrics also provide reporting requirements across key areas that are addressed during the evaluation of an agency's information security program.

The IG Metrics included 69 specific information security controls from NIST 800-53, Revision 4, to be tested for FY 2019 (see Appendix B for the complete list). The IG Metrics used for the FY 2019 FISMA evaluation are a continuation of work started in FY 2016 to develop and align the metrics within five functional areas: Identify, Protect, Detect, Respond, and Recover. These areas are within NIST's Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and align with both the federal IG and Chief Information Officer (CIO) metrics for related domains. These domains include Risk Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. FY 2019 is the first year in which both the IG and the CIO metrics were aligned across NIST's Cybersecurity Framework function areas (see Table 1).

Table 1: IG and CIO Metrics Align Across NIST Cybersecurity Framework Function Areas

Domain	Function Area
Risk Management	Identify
Configuration Management	Protect
Identity and Access Management	
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	Detect
Incident Response	Respond
Contingency Planning	Recover

Source: DHS.

[2] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

[3] A copy of the FY 2019 IG Metrics can be located online at https://www.cisa.gov/publication/fy19-fisma-documents (last accessed, March 31, 2020).

FISMA requires IGs to assess the effectiveness of their agency's information security programs on a maturity model spectrum in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent to which these policies are institutionalized. Within the context of the maturity model, a Level 4, Managed and Measurable, information security program is operating at an effective level of security. NIST provides additional guidance for determining the effectiveness of security controls.[4] When assessing the maturity of agencies' information security programs, IGs are to consider both their and management's assessment of the agency's missions, resources, and challenges. Table 2 details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized.

Table 2: IG Evaluation Maturity Levels

Maturity Level	Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized, and activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but implemented quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

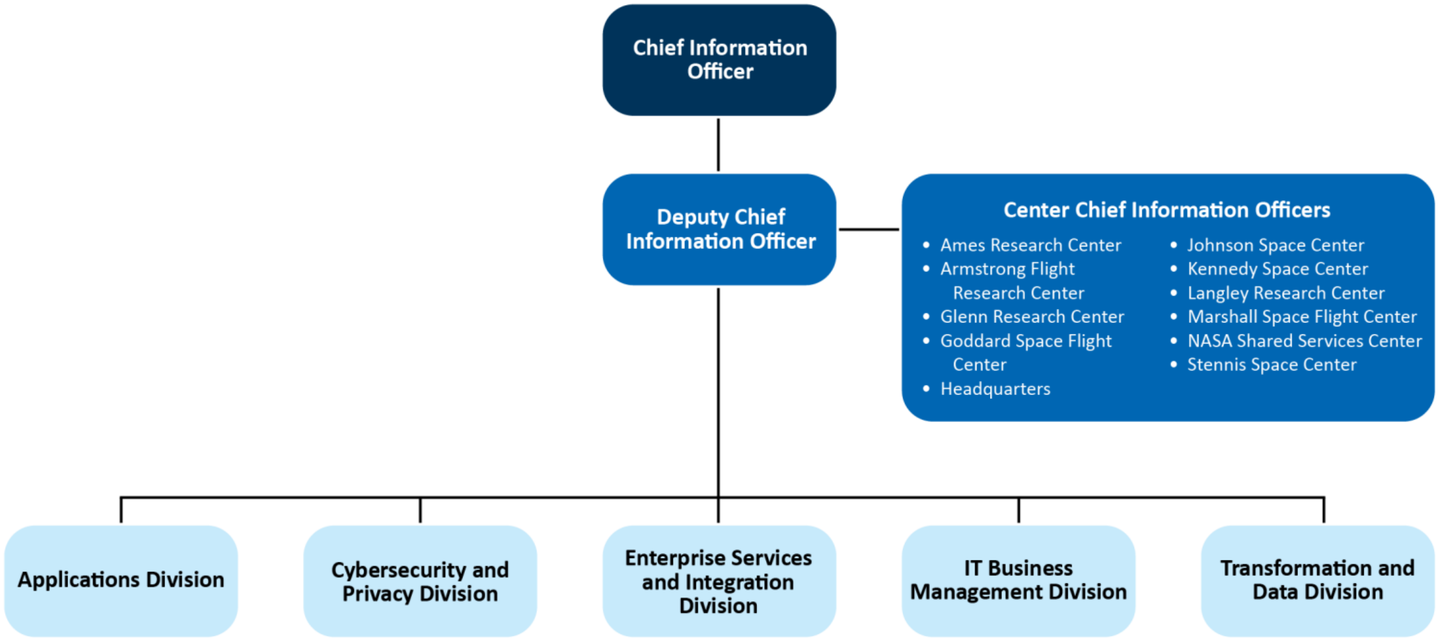
Source: DHS.

NASA Office of the Chief Information Officer

The CIO is responsible for ensuring the Agency's IT assets are acquired and managed in a manner consistent with federal policies, procedures, and legislation, including FISMA and the IG Metrics. The NASA Office of the Chief Information Officer (OCIO) has more than 175 professionals organized into five divisions: (1) Applications, (2) Cybersecurity and Privacy, (3) Enterprise Services and Integration, (4) IT Business Management, and (5) Transformation and Data. Figure 1 provides an overview of the OCIO's structure. For additional information about the OCIO organization and divisions, see Appendix C.

[4] NIST SP 800-53, Revision 4, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

Figure 1: Office of the Chief Information Officer Organizational Chart as of May 2020


Chief Information Officer
Deputy Chief Information Officer
Center Chief Information Officers
• Ames Research Center
• Armstrong Flight Research Center
• Glenn Research Center
• Goddard Space Flight Center
• Headquarters
• Johnson Space Center
• Kennedy Space Center
• Langley Research Center
• Marshall Space Flight Center
• NASA Shared Services Center
• Stennis Space Center
Applications Division
Cybersecurity and Privacy Division
Enterprise Services and Integration Division
IT Business Management Division
Transformation and Data Division

Source: NASA.

NASA Information Security Controls

NIST standards and guideline controls identify three types of information security controls: common, hybrid, and system specific. Common controls (also known as inherited controls) are controls that support multiple information systems. They are implemented and managed at the agency level but provide protections to systems throughout an agency. By centrally managing the development, implementation, assessment, authorization, and monitoring of common controls, information security costs can be amortized across multiple information systems. According to NIST, "many of the controls needed to protect organizational information systems (e.g., security awareness training, incident response plans, physical access to facilities, rules of behavior) are excellent candidates for common control status."[5]

At NASA, Agency-level common controls are aggregated and managed as a single system security plan (SSP) called the Agency Common Control (ACC) system that is maintained within the Agency's Risk Information Security Compliance System (RISCS).[6] The ACC system is implemented, documented, and maintained by staff in the OCIO with the CIO serving as the authorizing official (see Appendix C for more information on the authorizing official role). At the time our review, the ACC system consisted of both hybrid and non-hybrid common controls. Hybrid common controls have one component at the Agency level and another at the Center or system level. Responsibility for hybrid controls is shared between the OCIO and lower level IT management personnel. Non-hybrid common controls are those implemented and managed only at the Agency level and where responsibility rests solely with the OCIO. System-specific

[5] NIST SP 800-53, Revision 4.

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

controls are those that are applicable only to a single information system. Responsibility for system-specific controls belongs to the information system owner and the respective authorizing official.

Methods to Address Information Security Control Deficiencies

OMB, NIST, and NASA policies provide two alternative methods to address information security control deficiencies: (1) Plan of Action and Milestones (POA&M) or (2) Risk-Based Decision document.

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. According to OMB, a POA&M is intended to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.[7] 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."[8] POA&Ms—which serve as NASA's primary management tool to remediate information security-related weaknesses—are maintained in the RISCS database. The reports provide Agency information security officials with information to track and review progress on corrective actions. As of March 25, 2020, NASA had a total of 5,077 POA&Ms, which included, but was not limited to, 2,849 closed POA&Ms, 1,041 with milestones approved, 399 in draft, and 346 past due. POA&M reports also provide a basis for an authorizing official to revoke or approve 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. 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."[9]

Contingency Plans

Contingency planning for federal systems refers to the development of measures to recover information system services after a disruption occurs. In addition, contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the systems impact level. Consequently, operating an information system without the benefit of having a current, up-to-date contingency plan established could materially affect the Agency's ability to recover information systems in an effective and timely manner.

[7] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (October 17, 2001).

[8] NIST SP 800-53, Revision 4.

[9] ITS-HBK- 2810.02-02E, *Security Assessment and Authorization* (effective November 29, 2016).

NASA Information Security Progress and Fiscal Year 2019 FISMA Evaluation

Over the past 5 years, the OCIO has taken steps to improve NASA's overall information security program and posture, including implementing DHS and public law requirements as well as mandatory operational directives.[10] For example, NASA implemented RSA Archer, a commercial-off-the-shelf product used to manage and secure the Agency's information security documentation and institutionalize RISCS across the Agency. Additionally, NASA has been responsive in implementing audit recommendations issued by the Government Accountability Office and the OIG that have helped to improve the Agency's annual information security training. For example, in response to a NASA OIG recommendation, the Agency added information to the Agency's annual information security training to address IT supply chain risk management requirements and the acquisition and use of cloud computing services within NASA's network environments.[11] Although the Agency continues to make progress in securing its networks and information systems through these and other efforts, there remains significant opportunities for improvement. In the FY 2019 FISMA evaluation, we assessed NASA's information security program at a Level 2 and reported these results to OMB in October 2019.

To assess NASA's overall information security program for FY 2019, we examined NASA's information security policies, procedures, practices, and controls by examining six information systems. We chose these systems from a universe of more than 450 NASA and contractor information systems based on criteria, including Center in which the system was located, the system's Federal Information Processing Standards (FIPS) 199 category, and whether the system was NASA or contractor operated.[12] We also assessed the Agency's overall cybersecurity posture by using a variety of techniques that leveraged work previously performed by NASA, the OIG, and other oversight organizations. Table 3 provides a listing of the information systems examined during our evaluation.

Table 3: Information Systems Tested During FY 2019 FISMA Evaluation

Information System Descriptions	FIPS 199 Category	Organization Operated	Contractor Operated
Communications network	High	X	–
Critical system	High	–	X
Media system	Low	X	–
Research system	Moderate	X	–
Emergency system	Moderate	–	X
Commercial cloud computing service	Low	–	X

Source: NASA OIG.

Note: Specific names of the NASA information systems tested during this evaluation have been generalized to protect their operational security.

[10] DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products* (September 13, 2017) and Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. No. 113-6 (2013).

[11] NASA OIG, *Audit of NASA's Information Technology Supply Chain Risk Management Efforts* (IG-18-019, May 24, 2018).

[12] NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004). FIPS 199 provides a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction. The three levels are high, moderate, and low.

NASA's Information Security Program is Not Fully Integrated Across the Agency

NASA has not implemented an effective Agency-wide information security program. Specifically, we found SSP documentation for the Agency's information systems contained numerous instances of incomplete, inaccurate, or missing information, and the CIO has not addressed deficiencies in the ACC system—a system that impacts every NASA information system that inherits Agency common controls. FISMA requires federal agency CIOs to develop an agency-wide information security program, including setting information security policies, procedures, and controls. At NASA, the Chief Information Security Officers located at each Center are responsible for providing oversight to ensure that accurate records on the status of identified weaknesses, significant deficiencies, and nonconformance throughout the entire corrective action process are documented in RISCS. The issues we identified during this evaluation occurred primarily because the OCIO does not consistently require the use of RISCS as the Agency's information security management tool. Further, NASA information security personnel are not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that delinquent information security assessments are identified and mitigated. As a result, information systems throughout the Agency have inherited an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA's information.

Agency System Security Plans Contained Incomplete, Inaccurate, or Missing Information

To test the accuracy, adequacy, and sufficiency of NASA system security information, we reviewed SSP documentation recorded in RISCS for the six selected information systems. We found that all six SSPs contained incomplete, inaccurate, or missing information. Table 4 provides a listing of the issues identified when reviewing the SSPs.

Table 4: Incomplete, Inaccurate, or Missing SSP Information in RISCS

SSP Deficiencies in RISCS	System					
	1	2	3	4	5	6
SSPs not maintained in RISCS					●	●
Change in system owner not recorded						●
Security control assessments not performed or the dates not recorded		●	●		●	●
Justification for security control process deviations not provided	●	●	●	●	●	●
Missing or out-of-date boundary description					●	●
Control assessment implementation requirements referenced expired guidance	●	●	●			
Incorrect control assessment recorded			●			

Source: NASA OIG analysis.

NASA implemented RISCS to manage information system vulnerability, SSPs, and Continuous Diagnostics and Mitigation sensor information.[13] Centralized access to this information improves IT risk management and provides a consistent process for evaluating and improving the overall risk profile of the Agency's IT. Center Chief Information Security Officers provide oversight to help ensure that the information in RISCS is accurate; however, all six systems we tested had inaccurate or out-of-date information in RISCS. Our review of RISCS data found that required data fields (e.g., control risk assessment dates and assessment statuses), system security sections (e.g., system boundary descriptions), and other required SSP documentation (e.g., system components and contingency plans) were incomplete or outdated. This occurred because Center Chief Information Security Officers often are responsible for managing large portfolios of information systems and do not always have the resources available to ensure data in RISCS for each system is accurate and complete in a timely basis. We also found that RISCS permitted authorizing officials the ability to grant systems with the authority to operate despite missing or outdated data.

Further, we found instances where NASA information security personnel are not sufficiently aware of Agency procedural requirements for recording SSP information in RISCS. For example, the information system owners and authorization staff for two of the six systems we reviewed did not keep updated SSP information in RISCS because they are external systems.[14] While NASA guidance provides a simplified approach to the security assessment process for its external systems by allowing system owners to leverage assessments conducted by another entity, it still requires that any NASA-specific risk statements (e.g., a security assessment report on the status of the system's security controls) and authorization documents be stored in RISCS.[15] Additionally, according to the system owner and assessment staff, components of a third system's SSP in RISCS was not up-to-date because they were concerned that too many users had access to data stored in RISCS and felt that their system's information would not be adequately protected if kept there. Subsequently, we discussed their concerns with the OCIO officials who, while aware of the concern, stated that RISCS provides sufficient security as access to data in RISCS is based on a need-to-know and can be limited for a specific system.

Finally, documentation for SSPs does not accurately reflect the most current state of NASA's systems for elements such as information system controls, which can negatively affect the Agency's ability to secure, respond, and recover from information security events. For example, a security control for one of the six SSPs we reviewed was incorrectly assessed as "satisfied" based on a draft version of the system's contingency plan. As a result, the system owner and authorization staff took no mitigating action, and the system continued to operate within the NASA environment without a finalized and approved contingency plan for almost 2 years. Further, incomplete and inaccurate SSPs also limit the CIO's ability to adequately assess and monitor cybersecurity threats and risks to NASA information systems and make informed decisions affecting the Agency's overall information security posture. In turn, this could potentially result in the CIO developing policies and mitigating procedures that are not commensurate with the risk and magnitude of harm from malicious or unintentional impairment of the Agency's information systems and data.

[13] The Continuous Diagnostics and Mitigation Program is leading the effort to reduce cyber risk and provide visibility across the federal government.

[14] NASA defines external information systems as any information system owned, operated, and managed by outside agencies, contractors, universities, or other organizations that store, process, or disseminate NASA-owned data under a contract or formal agreement with the Agency.

[15] NASA ITS-HBK 2810.02-05A, *Security Assessment and Authorization: External Information Systems* (November 1, 2019).

NASA Has Not Fully Addressed Deficiencies in Agency Common Controls

During our review of the six information systems in our sample, we observed that each system had inherited information security controls that were part of the Agency's ACC system. However, many of those controls were classified as "other than satisfied," indicating they had been assessed as less than effective. Based on discussions with information system owners and other system security managers, system management personnel were unable to adequately explain the classification of ACCs or the Agency's plans to remedy assessed control weaknesses. Consequently, we performed a limited review of the Agency's ACC system in July 2019.

Agency Common Control System Deficiencies Have Not Been Addressed

Our limited review of the Agency's ACC system identified 203 common controls, of which NASA had assessed 94 (46 percent) as "other than satisfied." At the time of our review, the OCIO had not taken action to address the deficiencies. The following ACCs are examples of controls that NASA assessed as deficient, but had not been addressed with either (1) a POA&M detailing resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones, or (2) a Risk-Based Decision document providing analysis supporting the conclusion that a risk can be accepted without a corrective action plan:

- *Account Management—Disable Inactive Accounts*. The information system should automatically disable inactive accounts after 30 days.
- *Security Assessment and Authorization Policy and Procedures*. The organization develops, documents, and disseminates security assessment and authorization policy and implementation procedures that are annually reviewed and updated.
- *Malicious Code Protection—Automatic Updates.* The information system should automatically update malicious code protection mechanisms.

In 2019, we interviewed OCIO officials responsible for managing the ACC system and found that they were unaware of policies requiring that all "other than satisfied" controls be supported by a POA&M or Risk-Based Decision document.[16] Without these plans or documents to address known control deficiencies, the deficiencies will persist. As the ACCs affect information systems throughout the Agency, failure to properly address these deficiencies increases the risk of exploitations that threaten the confidentiality, integrity, and availability of NASA's information. For example, without controls in place to ensure that malicious code protection (e.g., anti-virus software) receives automatic updates, NASA information systems may be vulnerable to new and emerging threats.

While we support the updates that the OCIO has made to the ACC system, it is important to reiterate that without POA&Ms to address known control deficiencies NASA lacks corrective action plans and the deficiencies will persist. As the ACCs affect information systems throughout the Agency, failure to properly address these deficiencies increases the risk of exploitations that threaten the confidentiality, integrity, and availability of NASA's information.

[16] ITS-HBK- 2810.02-02E; NIST SP 800-53, Revision 4; and OMB Memorandum M-02-01.

NASA Has Addressed Some But Not All Control Deficiencies

In September 2019, the ACC authorizing official performed a security review for the purpose of reauthorizing the ACC system. The prior authorization for the ACC system had been in effect for 2 years and expired in March 2019. In preparing for the security review, OCIO officials elected to remove all hybrid common controls from the ACC system thereby reducing the total number of ACCs from 203 to 80. According to the security review documentation, after removing the hybrid controls the 40 remaining "other than satisfied" controls in the ACC system were properly supported by a POA&M or Risk-Based Decision document.[17]

When the hybrid common controls were removed from the ACC system, OCIO officials planned to aggregate them into a new system. According to the security review documentation, the new system of hybrid common controls was to become operational by the end of calendar year 2019. However, as of April 2020, NASA officials have not yet created this new system. Consequently, an unidentified number of "other than satisfied" hybrid common controls still have not been properly addressed by a POA&M or Risk-Based Decision document. Until a corrective action plan is developed for all hybrid common control deficiencies, the confidentiality, integrity, and availability of NASA information is at risk.

[17] We did not independently test the accuracy and completeness of the OCIO's security review documentation during this evaluation.

NASA Information Systems Operated Without Current or Available Contingency Plans

Of the six information systems reviewed, we found that four were operating without current or available contingency plans. While three of these four systems eventually updated their contingency plans in RISCS during the course of our evaluation, these systems had been operating under outdated plans for as long as 4 years. The fourth system is currently operating under a 2016 contingency plan. We are concerned that NASA practices allow information systems to function in an "operational" life-cycle status without a current, approved, and authorized contingency plan.

FISMA and NASA policies require that information systems include contingency plans containing policies and procedures that serve as a guide for enterprise response in the event of a loss of mission capability, ensure the availability of critical resources, and facilitate the continuity of operations in an emergency. Specifically, FISMA requires federal agencies to develop, document, and implement information security programs that support operations and assets to ensure continuity of operations for information systems that support the operations and assets of the agency.[18] Further, NASA policy requires information system owners to review contingency plans for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan.[19]

We found Agency authorizing officials and the CIO lacked adequate oversight of the contingency plan development, approval, and management process. Specifically, the authorizing officials are not performing regularly scheduled testing to determine that the information in RISCS is accurate, up to date, and usable by senior IT leadership. This system was categorized at a high level, meaning that the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.[20] The lack of current or available contingency plans puts NASA at an unnecessarily high level of risk by hindering the Agency's ability to recover information systems in an effective and efficient manner, thus threatening the confidentiality, integrity, and availability of NASA information maintained, processed, and stored in those systems.[21]

[18] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, (2014).

[19] NASA Procedural Requirements 2810.1A, *Security Information Technology (Revalidated with Change 1, dated May 19, 2011)* May 16, 2006.

[20] FIPS 199.

[21] NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

NASA's Process for Reviewing and Updating Information Technology Security Handbooks is Ineffective

During our review of OCIO IT security handbooks and other related IT governance documents, we found that 27 of 45 documents had not been reviewed and approved in more than 1 year and 8 that not been reviewed in over 3 years. OCIO policy states that IT security handbooks shall be reviewed or updated on an annual basis or more frequently if appropriate.[22] However, the OCIO policy management process does not provide adequate oversight of the policy review process or a reliable list of policies requiring review. OCIO officials stated that the Office intends to reengineer the review process in FY 2020 but expressed concern about the sufficiency of resources to complete this task. Failure to update NASA policy and procedures in a timely manner increases the risk that Agency personnel will employ out-of-date information security practices. We consider the timely review and update of IT governance documents to be a basic internal control necessary for the effective and efficient operation of Agency information systems.

NASA Information Technology Policies

NASA's IT policies consist of Agency-level directives and supplemental guidance issued by the OCIO with Agency-level directives such as NASA Policy Directives and NASA Procedural Requirements. These directives serve as the framework for lower-level supplemental guidance issued by the OCIO. As supplemental guidance, the OCIO develops, approves, and controls a catalog of IT security handbooks and other IT governance documents. This catalog of "other policy documents" is accessible through the NASA Online Directives Information System, and as of October 2019, they system contained 45 IT documents, including IT security handbooks, IT standard operating procedures, and one NASA information technology requirement.[23]

In 2018, NASA's policy review process for OCIO policies was outlined in an IT security handbook, which supplemented Agency-level directives. [24] The handbook assigned responsibilities, described a workflow for reviews and approvals, and required that IT governance documents be reviewed, updated, and approved annually. In October 2019, the OCIO issued a revised version of the handbook that maintained the review requirement and stated that IT security handbooks are "living" documents that should be reviewed/updated annually or more often if warranted.[25]

[22] ITS-HBK-2810-002.1C, *Format and Procedures for IT Security Policies and Handbooks* (effective October 2019).

[23] In addition to IT governance documents, the NASA Online Directives Information System library serves as the central repository for all Agency-level directives.

[24] ITS-HBK-0002C, *Format and Procedures for IT Security Policies and Handbooks* (effective July 13, 2018).

[25] ITS-HBK-2810-002.1C.

IT Security Handbooks Did Not Receive Timely Reviews

In October 2019, we reviewed the OCIO's catalog of IT security handbooks and other IT governance documents and found that 27 of the 45 documents (60 percent) had not been reviewed and approved in more than 1 year. Moreover, 8 of the 45 documents (18 percent) had not been reviewed and approved in more than 3 years.

NASA’s IT governance documents have not received timely reviews because the OCIO has not implemented an effective policy review and approval process. OCIO acknowledged that they have not maintained a complete and reliable listing of IT governance documents. They also acknowledged weaknesses in the policy review process and explained that the OCIO management plan for FY 2020 includes reengineering that process. However, the officials expressed concern about the sufficiency of resources needed for the reengineering because the activity will require the coordination and participation of a significant amount of personnel across the Agency.[26]

Issuing and maintaining current policies is a critical management function and a key component of an effective internal control system. Policies are used to communicate management's expectations regarding the Agency's IT environment and to assign roles and responsibilities for meeting NASA's IT security objectives. Policies are also used to reflect applicable federal laws, executive orders, directives, regulations, standards, and guidance. With the majority of IT security policies and procedures being out-of-date, the risk increases that Agency IT personnel will fail to secure IT systems in a manner that meets NASA's objectives and conforms to federal requirements. For example, without a current access control policy, NASA lacks assurance that access to the Agency’s information systems will be properly limited based on users’ need to know. We consider the OCIO’s failure to implement an effective policy management process as a weakness in the fundamental internal controls necessary for the effective and efficient operation of Agency information systems.

[26] NASA security personnel are located within the Agency’s mission directorates and Centers.

CONCLUSION

NASA's high-profile and sensitive technology makes the Agency an attractive target for computer hackers and other bad actors. Therefore, it is vital the Agency develop an integrated view of its information security program to protect the confidentiality, integrity, and availability of its data, systems, and networks. During this year's FISMA evaluation, NASA continued to make limited progress in securing its networks and information systems. However, issues with SSPs containing incomplete, inaccurate, or missing information, along with deficiencies identified in the ACC system, the management and administration of information system contingency plans, and ineffective processes for reviewing and updating IT security handbooks raises concerns about the overall robustness of the Agency's information security program. Consequently, in our view, the Agency's information security program remains at a Level 2, "Defined," when assessed against OMB's model of effectiveness. With the increasing threats facing NASA's information systems and networks, it is imperative the Agency continue its efforts to strengthen its risk management and governance practices to safeguard its data from cybersecurity threats.

Recommendations, Management's Response, and Our Evaluation

To strengthen the Agency's information security program, we made the following recommendations to the Acting Chief Information Officer:

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.
2. Implement a policy to enforce the Agency's requirement that RISCS be used as the main repository for all NASA SSPs and supporting documentation, including updated contingency plans, and that it accurately reflects the most current security state of NASA systems.
3. Perform an assessment to evaluate the feasibility of modifying RISCS to ensure that required data fields, system inventory sections, and other supporting documentation required for the creation or modification of an SSP are completed before a system can be authorized to operate.
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 to keep that data secure.
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.
6. Implement the necessary controls for the management of the hybrid common controls to include assessing control effectiveness and developing a POA&M or Risk-Based Decision document for every control assessed as "other than satisfied."
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.
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. At a minimum, these reviews should focus on any operational changes such as
   a. contingency planning policies and associated contingency planning controls,
   b. essential missions and business functions and associated contingency requirements,
   c. testing of the plan for the information system to determine the effectiveness of the plan and the organizational readiness to execute the plan,

   d. names and contact information of team members and vendors, and
   e. vital records (electronic and hardcopy).

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.

We provided a draft of this report to NASA management who concurred with the recommendations and described planned actions to address them. We consider management's comments responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the corrective actions.

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

Major contributors to this report include Mark Jenson, Financial Management Director; Joseph A. Shook, Project Manager; Sashka Mannion; Aleisha Fisher; James Pearce; Sarah McGrath; and Earl Baker.

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

Paul K. Martin
Inspector General

Appendix A: Scope and Methodology

We performed this evaluation from March 2019 through May 2020 in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency. 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.

To answer our objective and gain an understanding of the Agency's overall information security program and report the results to the Office of Management and Budget, we performed fieldwork at NASA Headquarters, Goddard Space Flight Center, Johnson Space Center, and Langley Research Center. The scope of this evaluation was NASA cybersecurity documentation and practices required by FISMA. Additionally, we reviewed six NASA information systems for compliance with FISMA requirements. To accomplish this, we interviewed OCIO officials, information system owners, information system security officers, security assessors, and Center OCIO staff. We analyzed the Agency's inventory of network and information systems. We also examined SSPs and tested information for existence, completeness, and accuracy to determine the adequacy of the Agency's information security efforts for six information systems operated by NASA or for the benefit of NASA. Additionally, we interviewed other Agency officials to gain an understanding of how NASA manages information security processes and procedures to protect the confidentially, integrity, and availability of NASA networks and information systems.

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. 111-352, *GPRA Modernization Act of 2010* (January 2011)
- 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)
- Binding Operation Directive 19-02 (BOD 19-02), *Vulnerability Remediation Requirements for Internet-Accessible Systems* (April 29, 2019)
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016)
- OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements* (October 25, 2018)
- OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 19, 2017)

- 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 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (August 2011)
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* (September 2008)
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (December 2014)
- 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 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003)
- NIST SP 800-39, *Managing Information Security Risk* (March 2011)
- 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 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010, Updated November 11, 2010)
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012)
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006)
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (April 16, 2018)

NASA Policy, Requirements, and Guidance

- NASA Policy Directive (NPD) 1001.0C, *2018 NASA Strategic Plan* (February 12, 2018)
- NPD 2810.1E, *NASA Information Security Policy* (January 31, 2020)
- NASA Procedural Requirements (NPR) 2810.1A, *Security Information Technology (Revalidated with Change 1, dated May 19, 2011)* (May 16, 2006)
- NPR 2800.1B, *Managing Information Technology* (March 20, 2009)
- NPR 1400.1H, *NASA Directives and Charters Procedural Requirements* (March 29, 2019)
- NPR 1600.1A, *NASA Security Program Procedural Requirements* (August 12, 2013)
- ITS-HBK 2810.04-01A, *Risk Assessment, Vulnerability Scanning, and Expedited Patching* (April 2019)

- 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 2810.09-02A, *NASA Information Security Incident Management* (November 1, 2019)
- ITS-HBK 2810.02-05A, *Security Assessment and Authorization: External Information Systems* (October 2016)

Use of Computer-Processed Data

We used computer-processed data to perform this evaluation, and that data was used to materially support findings, conclusions, and recommendations. To assess the quality and reliability of the data, we verified the information through independent calculations and corroboration with program documents and the input of various program officials. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

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 performed Agency-wide 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 report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 5 years, the NASA OIG and the Government Accountability Office have issued 44 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, respectively.

NASA Office of Inspector General

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)

NASA's Compliance with the Digital Accountability and Transparency Act of 2014 (IG-18-004, November 7, 2017)

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

NASA’s Efforts to Improve the Agency’s Information Technology Governance (IG-18-002, October 19, 2017)

Audit of Industrial Control System Security within NASA’s Critical and Supporting Infrastructure (IG-17-011, February 8, 2017)

Security of NASA’s Cloud Computing Services (IG-17-010, February 7, 2017)

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

Follow-up Evaluation of NASA’s Implementation of Executive Order 13526, Classified National Security Information (IG-16-030, September 28, 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)

Audit of the Spaceport Command and Control System (IG-16-015, March 28, 2016)

NASA's Management of the Near Earth Network (IG-016-014, March 17, 2016)

NASA's Efforts to Manage Its Space Technology Portfolio (IG-16-008, December 15, 2015)

Federal Information Security Management Act: Fiscal Year 2015 Evaluation (IG-16-002, October 19, 2015)

NASA's Management of the Deep Space Network (IG-15-013, March 26, 2015)

Government Accountability Office

Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed (GAO-20-126, December 12, 2019)

Information Technology: Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity (GAO-20-311T, December 11, 2019)

Information Security: VA and Other Federal Agencies Need to Address Significant Challenges (GAO-20-256T, November 14, 2019)

Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities (GAO-20-129, October 30, 2019)

Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid (GAO-19-332, August 26, 2019)

Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices (GAO-19-545, July 26, 2019)

Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384, July 25, 2019)

Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems (GAO-19-471, June 11, 2019)

Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288, May 17, 2019)

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

Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked (GAO-19-58, April 4, 2019)

Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs (GAO-19-144, March 12, 2019)

Internet Privacy and Data Security: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (GAO-19-427T, March 7, 2019)

Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption (GAO-18-211, February 15, 2018)

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)

Cybersecurity: Actions Needed to Strengthen U.S. Capabilities (GAO-17-440T, February 14, 2017)

Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely (GAO-17-163, February 1, 2017)

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

Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority (GAO-16-686, August 26, 2016)

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

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs (GAO-15-714, September 29, 2015)

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems (GAO-15-573T, April 22, 2015)

Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked (GAO-15-296, April 16, 2015)

APPENDIX B: INFORMATION SECURITY CONTROLS TESTED

Table 5: 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 (2) – Account Management | Removal of Temporary / Emergency Accounts		X	X
3	AC-08 – System Use Notification	X	X	X
4	AC-17 – Remote Access	X	X	X
5	AT-01 – Security Awareness and Training Policy and Procedures	X	X	X
6	AT-02 – Security Awareness Training	X	X	X
7	AT-03 – Role Based Security Training	X	X	X
8	AT-04 – Security Training Records	X	X	X
9	CA-01 – Security Assessment and Authorization Policy and Procedures	X	X	X
10	CA-02 – Security Assessments	X	X	X
11	CA-03 – System Interconnections	X	X	X
12	CA-05 – Plan of Action and Milestones	X	X	X
13	CA-06 – Security Authorization	X	X	X
14	CA-07 – Continuous Monitoring	X	X	X
15	CM-01 – Configuration Management Policy and Procedures	X	X	X
16	CM-02 – Baseline Configuration	X	X	X
17	CM-03 – Configuration Change Control		X	X
18	CM-06 – Configuration Settings	X	X	X
19	CM-07 – Least Functionality	X	X	X
20	CM-08 – Information System Component Inventory	X	X	X
21	CM-09 – Configuration Management Plan		X	X
22	CM-10 – Software Usage Restrictions	X	X	X
23	CP-01 – Contingency Planning Policy and Procedures	X	X	X
24	CP-02 – Contingency Plan	X	X	X
25	CP-03 – Contingency Training	X	X	X
26	CP-04 – Contingency Plan Testing	X	X	X
27	CP-06 – Alternate Storage Site		X	X
28	CP-07 – Alternate Processing Site		X	X
29	CP-08 – Telecommunications Services		X	X
30	CP-09 – Information System Backup	X	X	X
31	IA-01 – Identification and Authentication Policy and Procedures	X	X	X
32	IR-01 – Incident Response Policy and Procedures	X	X	X
33	IR-04 – Incident Handling	X	X	X
34	IR-06 – Incident Reporting	X	X	X
35	IR-07 – Incident Response Assistance	X	X	X
36	MP-03 – Media Marking		X	X

#	Information Security Control	FIPS 199 Security Category		
		Low	Moderate	High
37	MP-06 – Media Sanitization	X	X	X
38	PL-02 – SSP	X	X	X
39	PL-04 – Rules of Behavior	X	X	X
40	PL-08 – Information Security Architecture		X	X
41	PS-01 – Personnel Security Policy and Procedures	X	X	X
42	PS-02 – Position Risk Designation	X	X	X
43	PS-03 – Personnel Screening	X	X	X
44	PS-06 – Access Agreements	X	X	X
45	PM-05 – Information Inventory	Independent of any system impact level		
46	PM-07 – Enterprise Architecture			
47	PM-08 – Critical Infrastructure Plan			
48	PM-09 – Risk Management Strategy			
49	PM-11 – Mission/Business Process Definition			
50	RA-01 – Risk Assessment Policy and Procedures	X	X	X
51	RA-02 – Security Categorization	X	X	X
52	AR-04 – Privacy Monitoring and Auditing (Appendix J)	X	X	X
53	AR-05 – Privacy Awareness and Training (Appendix J)	Independent of any system impact level		
54	SA-03 – System Development Life Cycle			
55	SA-04 – Acquisition Process	X	X	X
56	SA-08 – Security Engineering Principles		X	X
57	SA-09 – External Information System Services	X	X	X
58	SA-12 – Supply Chain Protection			X
59	SC-07 (10) – Boundary Protection | Prevent Unauthorized Exfiltration			
60	SC-08 – Transmission Confidentiality and Integrity		X	X
61	SC-18 – Mobile Code		X	X
62	SC-28 – Protection of Information at Rest		X	X
63	SI-02 – Flaw Remediation	X	X	X
64	SI-03 – Malicious Code Protection	X	X	X
65	SI-04 – Information System Monitoring	X	X	X
66	SI-04 (4) – Information System Monitoring | Inbound and Outbound Communications Traffic		X	X
67	SI-04 (18) – Information System Monitoring | Analyze Traffic / Covert Exfiltration			
68	SI-07 (8) – Software, Firmware, and Information Integrity | Auditing Capability for Significant Events			
69	SE-02 – Privacy Incident Response (Appendix J)	Independent of any system impact level		

Source: NIST SP 800-53, Revision 4.

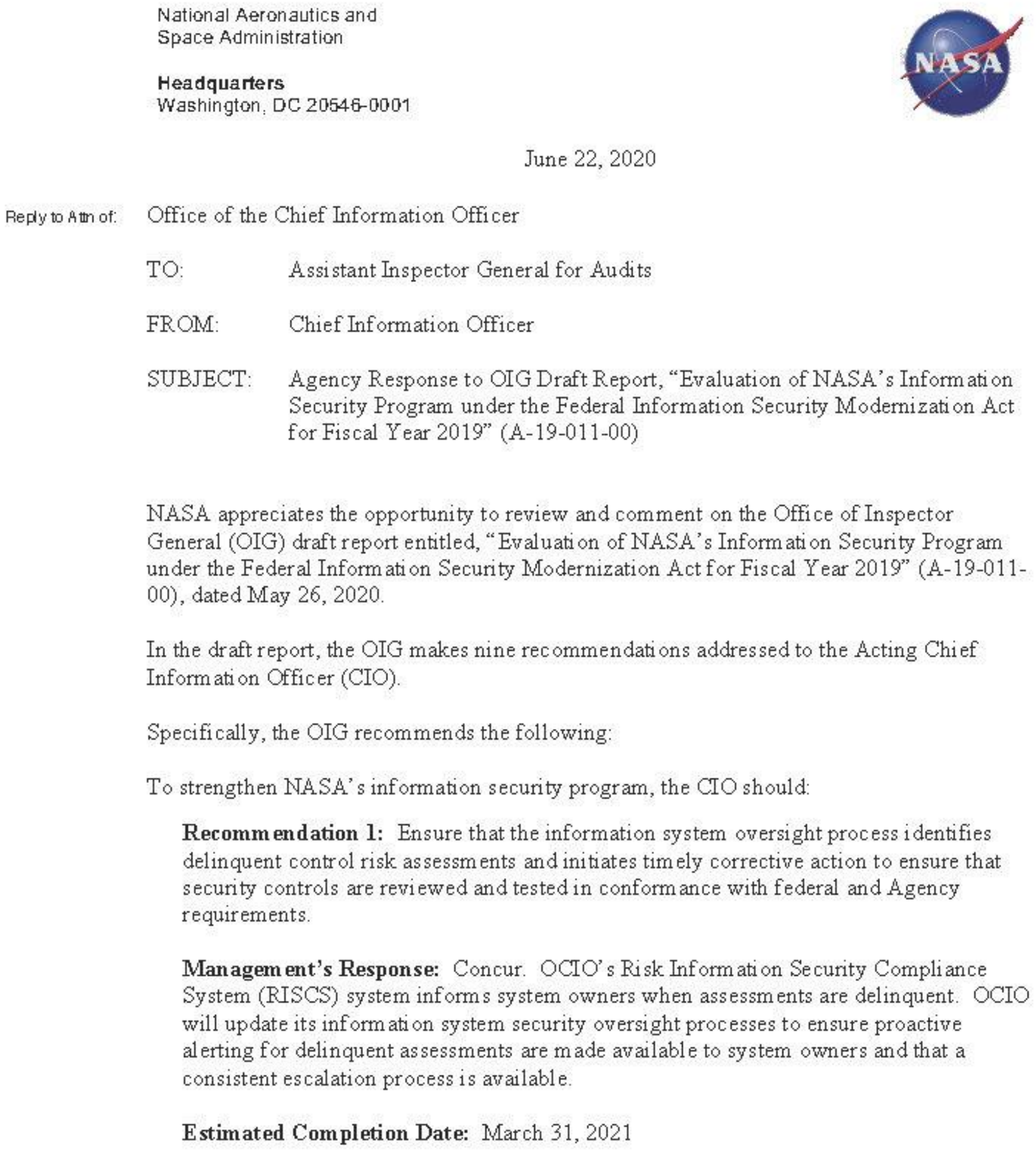
Appendix C: Office of the Chief Information Officer Organization and Roles

Table 6: Office of the Chief Information Officer Division and Security Role Descriptions

Division/Position	Description
OCIO Divisions	
Applications Division	Manages the planning, design, integration, and delivery of NASA's enterprise applications projects and services across the Agency.
Cybersecurity and Privacy Division	Manages the Agency-wide information and information security program in support of NASA's information systems and e-Gov initiatives.
Enterprise Services and Integration Division	Develops, maintains, and facilitates the implementation of the NASA Enterprise Architecture and delivery of IT infrastructure elements.
IT Business Management Division	Administers NASA's IT strategic planning process, and operational activities.
Transformation and Data Division	Guides NASA's data strategy, strategic investment decisions, and identifies emerging IT technologies to best support NASA's technology needs.
OCIO Security Roles	
Chief Information Officer	Agency official responsible for providing advice and other assistance to the head of the executive agency and other senior management personnel and is responsible for promoting the effective and efficient design and operation of all major information resources management processes for the agency.
Chief Information Security Officers	Officials who execute the responsibilities of the Senior Agency Information Security Officer as applicable at the Center level. Ensuring compliance with information security requirements relative to all personnel, information and information systems that are resident at, or managed from their Center. Individuals are responsible for the oversight of information security operations, and governance to ensure compliance with federal and NASA information security requirements.
Authorizing officials	Agency officials with the authority to assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
Information system owners	Individuals responsible for activities including but not limited to the acquisition, operation, maintenance, and disposal of information systems. Ensuring system-level implementation of Agency and Center requirements, while ensuring that security controls are implemented according to a thorough risk-based analysis of their information systems' security postures.
Information System Security Officers	Individuals with assigned responsibilities for maintaining the appropriate operational security posture for an information system or program, and are responsible for the day-to-day security operations of the information system.
Security control assessors	Individuals, groups, or organizations responsible for the performance of assessments of system security controls to determine the overall effectiveness of security and privacy controls associated with information system.

Source: OCIO and NIST.

APPENDIX D: MANAGEMENT'S COMMENTS



National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

June 22, 2020

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, "Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019" (A-19-011-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019" (A-19-011-00), dated May 26, 2020.

In the draft report, the OIG makes nine recommendations addressed to the Acting Chief Information Officer (CIO).

Specifically, the OIG recommends the following:

To strengthen NASA's information security program, the CIO should:

Recommendation 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.

Management's Response: Concur. OCIO's Risk Information Security Compliance System (RISCS) system informs system owners when assessments are delinquent. OCIO will update its information system security oversight processes to ensure proactive alerting for delinquent assessments are made available to system owners and that a consistent escalation process is available.

Estimated Completion Date: March 31, 2021

Recommendation 2: Implement a policy to enforce the Agency's requirement that RISCS be used as the main repository for all NASA System Security Plans (SSPs) and supporting documentation, including updated contingency plans, and that it accurately reflects the most current security state of NASA systems.

Management's Response: Concur. As of November 1, 2019, OCIO updated its policy handbook ITS-HBK-2810.02-02E, *Security Assessment & Authorization,* to state that RISCS is the authoritative tool and solution for documenting all activities associated with the risk management framework. The policy update further clarifies the responsibility of the Authorizing Official and the Information System Owner to document risk-based decisions, security control implementation details, and authorization decisions for associated SSPs in RISCS. The update also highlights the responsibility of the information system owner to ensure that the authorization package in RISCS is regularly updated to reflect current configurations, control implementations, and the environment of the system.

Estimated Completion Date: Completed

Recommendation 3: Perform an assessment to evaluate the feasibility of modifying RISCS to ensure that required data fields, system inventory sections, and other supporting documentation required for the creation or modification of an SSP are completed before a system can be authorized to operate.

Management's Response: Concur. OCIO will evaluate the feasibility of modifying RISCS to include additional pre-requisite required fields before an Authority to Operate (ATO) can be submitted for approval to an Authorizing Official.

Estimated Completion Date: January 15, 2021

Recommendation 4: Update the current training for system owners and system assessment and authorization staff that covers the requirements for maintaining SSPs and supporting plan documentation in RISCS, as well as RISCS's data protection capabilities to keep that data secure.

Management's Response: Concur. OCIO will update its role-based training for information system owners, information system security officers, and authorizing officials to clarify policy requirements for maintaining authorization package documentation in RISCS.

Estimated Completion Date: October 29, 2021

Recommendation 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 Plan of Actions and Milestones (POA&M) or Risk-Based Decision document and track exceptions in Agency-wide monitoring tools.

Management's Response: Concur. OCIO will update its policy handbooks to ensure that "other than satisfied" controls are properly addressed by a POA&M or Risk-Based Decision in RISCS.

Estimated Completion Date: March 15, 2021

Recommendation 6: Implement the necessary controls for the management of the hybrid common controls to include assessing control effectiveness and developing a POA&M or Risk-Based Decision document for every control assessed as "other than satisfied."

Management's Response: Concur. OCIO is in the process of updating its hybrid controls system package and will document POA&Ms or Risk-Based Decisions for "other than satisfied" controls.

Estimated Completion Date: January 15, 2021

Recommendation 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.

Management's Response: Concur. OCIO will update its policy guidance for security control selection to clarify the requirements that if control CP-2 Contingency Plan is part of a system's control baseline but is deemed not applicable, a justification must be documented in RISCS. Per recommendation 5, OCIO will update its policy handbooks to ensure that any "other than satisfied" controls are properly addressed by a POA&M or Risk-Based Decision in RISCS.

Estimated Completion Date: March 15, 2021

Recommendation 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. At a minimum, these reviews should focus on any operational changes such as:

a. contingency planning policies and associated contingency planning controls,
b. essential missions and business functions and associated contingency requirements,
c. testing of the plan for the information system to determine the effectiveness of the plan and the organizational readiness to execute the plan,
d. names and contact information of team members and vendors, and
e. vital records (electronic and hardcopy).

Management's Response: Concur. OCIO will update its policy guidance for security control selection to clarify the requirements that if control CP-2 Contingency Plan is part of a system's control baseline but is deemed not applicable, a justification must be documented in RISCS. Per recommendation 5, OCIO will update its policy handbooks to ensure that any "other than satisfied" controls are properly addressed by a POA&M or Risk-Based Decision in RISCS.

Estimated Completion Date: March 15, 2021

Recommendation 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.

Management's Response: Concur. OCIO is in the process of updating its policy management process to ensure security handbooks and guidance documents are regularly updated as needed.

Estimated Completion Date: January 15, 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: 2020.06.23 08:45:07 -04'00'

Jeff Seaton
Chief Information Officer (Acting)

APPENDIX E: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Acting Chief Information Officer
Associate Chief Information Officer for Cybersecurity and Privacy

Non-NASA Organizations and Individuals

Office of Management and Budget
  Deputy Associate Director, Energy and Space Programs Division

Government Accountability Office
  Director, Contracting and National Security Acquisitions
  Director, Information Technology and Cybersecurity

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies

Senate Committee on Commerce, Science, and Transportation
  Subcommittee on Aviation and Space

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Reform
  Subcommittee on Government Operations

House Committee on Science, Space, and Technology
  Subcommittee on Investigations and Oversight
  Subcommittee on Space and Aeronautics

(Assignment No. A-19-011-00)