NASA OFFICE OF INSPECTOR GENERAL

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

April 14, 2016

TO: Renee P. Wynn
Chief Information Officer

SUBJECT: Final Memorandum, *Review of NASA's Information Security Program* (IG-16-016; A-15-005-01)

Dear Ms. Wynn,

As part of our annual review of NASA's compliance with the Federal Information Security Management Act of 2002 (FISMA) for fiscal year 2015, we reviewed a representative sample of 29 information systems from NASA Centers, Headquarters, and the Jet Propulsion Laboratory (JPL) and issued a summary report in October 2015.[1] In that report, we concluded that although NASA had established programs to address each of the review areas identified by the Department of Homeland Security's (DHS) FISMA guidance, the Agency needed to enhance its efforts in three areas: continuous monitoring management, configuration management, and risk management. We believe that weaknesses in these areas stem from missing requirements related to the Agency's information system security program. This report focuses on whether NASA has implemented programmatic, Agency-wide information security requirements that are independent of any particular information system. See Enclosure I for details on the scope and methodology.

[1] NASA Office of Inspector General, "Federal Information Security Management Act: Fiscal Year 2015 Evaluation" (IG-16-002, October 19, 2015).

Background

NASA depends on information technology and the information systems developed from that technology to carry out its missions and business functions. As highlighted by recent data breaches at the Office of Personnel Management and the Internal Revenue Service, Federal agencies face an evolving cybersecurity landscape.[2]

To improve cybersecurity and address the increasing sophistication of attacks, the Government relies on a variety of initiatives. First, FISMA requires Federal agencies maintain an information security program commensurate with their risk profile.[3] Second, the National Institute of Standards and Technology (NIST) issues security standards and guidelines for information systems utilized by Federal agencies. Finally, as the operational lead for Federal civilian cybersecurity, DHS operates a number of protection programs on behalf of the Government.

FISMA Requirements for an Information Security Program

FISMA requires that NASA develop, document, and implement an Agency-wide information security program and that the Agency Chief Information Officer (CIO) designate a Senior Agency Information Security Officer (Senior Security Officer) to assist NASA with this responsibility.

NIST Requirements for Program Management Controls

NIST specifies the requirements for program management controls and provides guidelines for assessing Agency-wide information security programs.[4] Management controls, which are typically implemented at the organization level rather than directed at individual information systems, help facilitate compliance with applicable Federal laws, Executive orders, directives, policies, regulations, and standards. Examples of management controls include an organization's information security program plan, Senior Security Officer, risk management framework, information security architecture, insider threat program, and critical infrastructure plan. See Enclosure II for the list of NIST-suggested management controls.

Government-wide Programs Administered by DHS

DHS helps Federal agencies protect their information systems by deploying initiatives such as the Continuous Diagnostics and Mitigation (CDM) program, vulnerability scanning, and the Trusted Internet Connections Initiative.

The CDM program is expected to provide Federal agencies with commercial off-the-shelf tools that enable system and network administrators to identify cybersecurity risks related to their networks, including current vulnerabilities and configuration settings. Having this information should allow

[2] In June 2015, the Office of Personnel Management reported an intrusion into its systems that affected the personnel records of about 4 million current and former Federal employees. In June 2015, the Internal Revenue Service Commissioner testified that unauthorized third parties had gained access to taxpayer information, including Social Security numbers, dates of birth, and street addresses, for approximately 100,000 tax accounts.

[3] The 2002 FISMA Act was amended by the Federal Information Security Modernization Act of 2014 on December 18, 2014.

[4] NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, and NIST Special Publication 800-53A, Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," December 2014.

agencies to prioritize and mitigate problems on an on-going basis. In September 2015, DHS awarded a task order to Booz Allen Hamilton (Booz Allen) to implement CDM services at NASA and several other Federal agencies. NASA officials are working with Booz Allen to integrate the necessary information security tools for deployment.

DHS also conducts network and vulnerability scans of Federal agencies' publicly accessible systems.[5] As a result of this activity, DHS generates a weekly "Cyber Hygiene" report for each agency describing the vulnerabilities detected, identifying the affected systems, and providing guidance regarding mitigation. In recognition of increased cyber threats to Government systems, in May 2015, DHS mandated that Federal agencies mitigate all critical vulnerabilities in publicly accessible systems within 30 days.[6] NASA generally meets this timeframe.

DHS also oversees the Trusted Internet Connections Initiative designed to consolidate external access points, including connections to the internet across the Federal Government. Since 2009, NASA adopted and has managed the Trusted Internet Connections Initiative's hardware – the National Cybersecurity Protection System (also known as EINSTEIN) – to monitor and analyze internet traffic as it moves through the Agency's networks.

NASA NEEDS IMPROVED MANAGEMENT CONTROLS TO STRENGTHEN ITS INFORMATION SECURITY PROGRAM

Although NASA has made progress in meeting requirements in support of an Agency-wide information security program, it has not fully implemented key management controls essential to managing that program. Specifically, NASA lacks an Agency-wide risk management framework for information security and an information security architecture. In our judgment, this condition exists because the Office of the CIO (OCIO) has not developed an information security program plan to effectively manage its resources. In addition, the Office is experiencing a period of transition with different leaders acting in the Senior Security Officer role, which has caused uncertainty surrounding information security responsibilities at the Agency level. As a result, we believe NASA's information security program could be improved to more effectively protect critical Agency information and related systems.

Efforts to Implement an Information Security Program

NASA has established an Agency information security program and implemented management controls to support that program. The OCIO leads the information security program and implements the program in conjunction with the Office of Protective Services (OPS).

[5] Office of Management and Budget Memorandum M-15-01, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices," October 3, 2014.

[6] DHS Binding Operational Directive 15-01 "Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems," May 21, 2015.

Office of the Chief Information Officer

The Senior Security Officer is responsible for leading the OCIO's Information Technology Security Division. During the past decade, the Information Technology Security Division has implemented several requirements for the Agency's information security program:

- As far back as 2005, Booz Allen began assessing the security risk associated with selected systems at NASA Centers. The assessment included penetration testing to simulate sophisticated hacker techniques to the greatest extent possible without adversely impacting operational NASA systems or networks.

- In 2006, NASA established the certification and accreditation process (which has evolved into the current assessment and authorization processes) at the system and Center level.

- In 2008, NASA established the Security Operations Center (SOC) at Ames Research Center to strengthen the Agency's ability to detect and respond to cyber attacks. The SOC continuously monitors traffic entering and leaving NASA computer systems using a variety of intrusion detection and prevention tools. In addition, the SOC coordinates, tracks, and reports information technology security incidents Agency-wide.

- In 2012, NASA established the Web Application Security Program to identify and assess vulnerabilities on the Agency's publicly accessible web applications and to mitigate the most significant of those vulnerabilities. As part of Web Application Security Program, NASA hired Booz Allen to conduct automated scans on a quarterly basis and monthly manual testing of Agency web applications to identify, categorize, and track vulnerabilities.

- In 2013, the Ames Research Center led the team that started an ongoing phishing exercise for the Agency on behalf of the Information Technology Security Division. The exercise is undertaken every quarter and potentially on every user, with the goal of increasing awareness of information technology security issues. This exercise is in response to indications that phishing is the number one attack vector for NASA.

- In 2015, NASA established the Blue Team Vulnerability Assessment Program to examine the operational security posture of the Agency's critical mission systems and networks. JPL initiated the effort in 2014 by inviting TASC (formerly known as The Analytic Sciences Corporation) to review the cyber security measures protecting some of its critical mission systems. TASC has performed multiple reviews of space mission operations, including high security missions with the National Reconnaissance Office and other Federal agencies. The OCIO, in collaboration with NASA's Office of Safety and Mission Assurance, obtained funding for TASC and a team from NASA's Independent Verification and Validation Facility performed the assessment at JPL in 2015. The assessment will continue through fiscal year 2018 and include visits to Goddard Space Flight Center, Johnson Space Center, and Marshall Space Flight Center.

Office of Protective Services

OPS supports the OCIO in protecting the Agency's information security program. The Office is also responsible for the insider threat program, critical infrastructure plan, and threat awareness program.

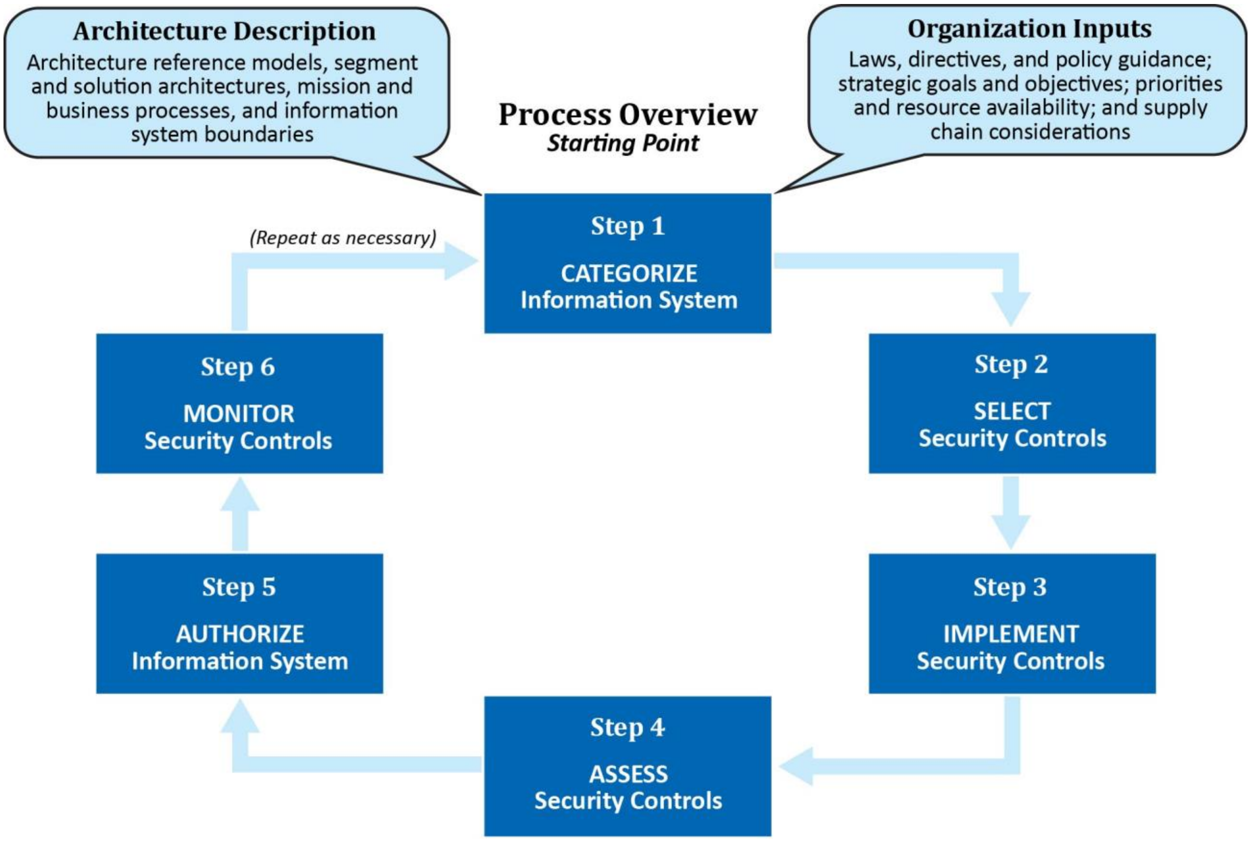
Risk Management Framework and Information Security Architecture

Despite the efforts outlined previously, NASA lacks an Agency-wide risk management framework for information security or an information security architecture. In 2015, the Agency identified these deficiencies as a part of its Business Services Assessment and pledged to correct them in 2016.

Risk Management

Risk management is a comprehensive process that requires an organization to describe the environment in which it makes decisions to assess, respond to, and monitor risk over time. As illustrated in Figure 1, a risk management framework provides a disciplined and structured process that integrates information security and risk management activities into the development life cycle of information technology systems.

Figure 1: Risk Management Framework


Architecture Description
Architecture reference models, segment and solution architectures, mission and business processes, and information system boundaries
Organization Inputs
Laws, directives, and policy guidance; strategic goals and objectives; priorities and resource availability; and supply chain considerations
Process Overview
Starting Point
Step 1
CATEGORIZE Information System
(Repeat as necessary)
Step 2
SELECT Security Controls
Step 3
IMPLEMENT Security Controls
Step 4
ASSESS Security Controls
Step 5
AUTHORIZE Information System
Step 6
MONITOR Security Controls

Source: NASA Office of Inspector General presentation of NIST information.

NASA policy defines a risk management framework as a concept that focuses on near real-time risk management, continuous monitoring of information security postures, the automation and enterprise consolidation of common security objectives, and the selection, implementation, assessment, and monitoring of security controls. The most critical underlying feature of a risk management framework is the concept that security practices are governed by a balanced understanding of information security postures and the impact of potential compromise on the Agency's mission needs and objectives.[7]

To integrate an agency-wide risk management framework, a three-tiered approach that addresses risk at the organization level, mission/business process level, and information system level is generally employed.[8] Tier 1 addresses risks from an organizational perspective and provides a prioritization of mission/business functions, which in turn drive investment strategies and funding decisions affecting the development of enterprise architecture at tier 2 and the allocations and deployment of management, operational, and technical security controls at tier 3. While NASA has a risk management framework at the system and Center levels (tier 3), it lacks a tier 1, Agency-wide risk management framework for information security.

In our FISMA reviews for fiscal years 2011 through 2015, we reported OCIO officials had not developed an Agency-wide risk assessment process specific to information security. In addition, in six other audits over the past 5 years, we identified areas in which NASA could improve its risk management program.[9] Without an Agency-wide risk management framework, NASA cannot obtain reasonable assurance that risk accepted at the system and Center levels would also be acceptable at the Agency level.

Information Security Architecture

According to NIST, integration of information security requirements and associated security controls into an enterprise architecture helps ensure organizations address security considerations early in the system development life cycle and that resulting controls are directly and explicitly related to an organization's mission and/or business processes.[10] The integration process also embeds into an organization's enterprise architecture an integral information security architecture consistent with organizational risk management and information security strategies. The information security architecture is developed at a system-of-systems level (organization-wide), representing all of an organization's information systems.

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

[8] NIST Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

[9] NASA Office of Inspector General, "Audit of the Space Network's Physical and Information Technology Security Risks" (IG-14-026, July 22, 2014); "Security of NASA's Publicly Accessible Web Applications" (IG-14-023, July 10, 2014); "NASA's Management of its Smartphones, Tablets, and Other Mobile Devices" (IG-14-015, February 27, 2014); "NASA's Progress in Adopting Cloud-Computing Technologies" (IG-13-021, July 29, 2013); "NASA's Information Technology Governance" (IG-13-015, June 5, 2013); and "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-017, March 28, 2011).

[10] NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

The primary purpose of an enterprise architecture at NASA is to align all aspects of the Agency's business, financial, scientific, and engineering needs with its technology infrastructure and resources to improve the performance of information technology and support Agency missions. The Agency-wide information security architecture is integral to and developed as part of the enterprise architecture.[11]

As of February 2016, NASA officials had assigned resources and began making progress documenting the Agency's information security architecture. While not yet complete, we believe taking this step would help NASA better determine how to effectively invest its resources to ensure security considerations are addressed early in the system development life cycle and the resulting controls are directly and explicitly related to NASA's missions.

Business Services Assessment

NASA has identified deficiencies in its risk management framework and information security architecture. In 2014, the Agency embarked on an effort to address the technical capabilities required to support NASA goals from a strategic perspective. Referred to as the Technical Capabilities Assessment Team, this effort aimed to provide NASA leadership with the information needed to make informed decisions about investing and divesting in capabilities to ensure the Agency has the appropriate mix of personnel and assets to carry its mission forward.

As the follow-on step to the Technical Capabilities Assessment Team, NASA expanded the assessment to include business and mission support services (referred to as the Business Services Assessment). The Business Services Assessment is designed to use a disciplined approach to strategically assess business and mission support services, including the current health of the services as well as opportunities for optimization.

As a part of the Business Services Assessment, NASA completed a review of information security in 2015 and concluded the Agency lacks an enterprise-wide risk management framework. As a result, the Mission Support Council (Council) tasked the OCIO's Information Technology Security Division with establishing an Agency information security risk management framework and an information security architecture by November 2015.[12] Although the OCIO made progress by providing resources and establishing plans to accomplish these tasks, they remain incomplete as of February 2016. The Information Technology Security Division planned to update the Council on its efforts at the group's March 2016 meeting. We plan to follow up with the Council to ensure these tasks are completed.

[11] NIST defines information security architecture as an integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, and personnel and organizational subunits, and shows their alignment with the enterprise's mission and strategic plans. Enterprise architecture is a strategic information asset base that defines the mission, the information and technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. In addition, enterprise architecture includes a baseline architecture, target architecture, and sequencing plan.

[12] The Mission Support Council serves as the Agency's senior decision-making body regarding the integrated Agency mission support portfolio. The Council determines mission support requirements to enable the accomplishment of the Agency's mission.

Information Security Program Plan

Developing an information security risk management framework and architecture is a complex undertaking that requires agency-wide involvement, from senior leaders who provide the strategic vision and top-level goals and objectives, to mid-level leaders who plan and manage projects, to individuals on the front lines who operate the systems that support an organization's core missions and business processes. We believe an information security program plan for NASA would help link the risk management processes at the system levels to those at the Agency level and provide essential information to help facilitate decision making regarding the acceptance of appropriate levels of risk.

According to NIST, Federal agencies must develop and disseminate an organization-wide information security program plan to identify requirements for the information security program. Specifically, the plan needs to

- provide a description of the management controls and common controls in place or planned for meeting those requirements;
- include identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities responsible for different aspects of information security (e.g., physical and personnel), and compliance;
- define the frequency for reviews of the security program plan; and
- receive approval from a senior official with responsibility and accountability for the risk being incurred.[13]

An organization-wide information security program plan, together with the security plans for individual information systems, provide coverage for all security controls employed within an organization. At the discretion of agencies, the information security program plan may be represented in a single document or a compilation of documents. If the information security program plan contains multiple documents, an organization should specify in each the official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective controls. For example, an organization may require that its facilities management office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls supporting multiple information systems.

We found NASA has not developed or disseminated an Agency-wide information security program plan. Although the OCIO has a separate document for Agency common controls, the document is not clear regarding roles and responsibilities, including who authorized the plan and the frequency with which controls should be reviewed and tested.[14] As a result, accountability is not clearly established and there is no assurance that program management and common controls are subject to the same authorization, assessment, and monitoring requirements as security controls at the system level.

[13] Common controls are security controls whose implementation results in a security capability that is inheritable by one or more of an organization's information systems. Examples of common controls include physical and environmental protection controls, security awareness training, incident response plans, physical access to facilities, and vulnerability scanning.

[14] The OCIO's Information Technology Security Division has a system security plan named the "NASA Agency Common Controls."

Without a comprehensive information security program plan, we believe NASA will continue to struggle to identify the resources needed to implement requirements for its information security program, including the risk management framework and information security architecture.

Senior Security Officer

NASA policies require the Senior Security Officer to serve as the Information System Risk Executive responsible for ensuring that security risk-related considerations and risk management of individual information systems are consistent across the Agency, viewed from an Agency-wide and strategic goal perspective, and reflect the Agency's risk tolerance affecting mission/business success. In addition, the Senior Security Officer is responsible for developing a NASA-wide information security program, including the risk management strategy and enterprise security architecture. Finally, the Senior Security Officer is responsible for continuously reviewing the information security program and establishing a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA's information security program.

As of February 2016, NASA did not have a permanent Senior Security Officer and three different employees have served as the acting Senior Security Officer over the previous 19 months. We believe the absence of a permanent Senior Security Officer has contributed to uncertainty regarding the position's responsibilities and resulted in a lack of strong leadership to manage the information security program.

CONCLUSION

Although NASA has made progress in implementing security controls and aspects of its information security program, we believe the program would be more effective were it managed in accordance with NIST management controls. NASA's high profile and sensitive technology makes the Agency an attractive target for hackers, and it is vital the Agency develop an integrated view of its information security program to protect its data and resources.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To improve management of NASA's information security program, we recommended the NASA CIO direct the Senior Security Officer to develop and disseminate an Agency-wide information security program plan that meets NIST requirements.

We provided a draft of this memorandum to NASA management for review and comment. Management concurred with our recommendation and described corrective actions to address it. We consider management's comments responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed corrective actions. NASA's full response is reproduced in Enclosure III. Technical comments provided by the Agency have also been incorporated, as appropriate.

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.

Sincerely,

Paul K. Martin
Inspector General

cc: Joseph Mahaley
Assistant Administrator for Protective Services

Enclosures – 3

Enclosure I: Scope and Methodology

We performed this review from February 2015 through March 2016 in accordance with the *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the review to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

For this review, we evaluated whether NASA complied with fiscal year 2015 FISMA requirements and the effectiveness of NASA's information security program. We followed the instructions dated December 14, 2014, from DHS's Office of Cybersecurity and Communications. We reviewed a sample of 29 Agency and contractor information systems for compliance with FISMA requirements. We reviewed relevant documentation, including information system security plans, risk assessment reports, security assessment reports, and accreditation decision letters; however, we did not evaluate the technical adequacy of these documents other than to determine whether they generally met Office of Management and Budget (OMB) and NIST guidelines. In addition, we interviewed NASA security officials and staff at NASA Headquarters, Centers, and JPL. We also determined whether deficiencies identified in the fiscal year 2014 FISMA review continue to exist. Further, we assessed the impact of recently completed or ongoing NASA OIG audits. Lastly, we performed work to address fiscal year 2015 DHS requirements within the 10 areas we reviewed.

We reviewed the following Federal and Agency criteria, policies, and procedures:

- Pub. L. No. 107-347, "E-Government Act of 2002," December 2002
- Pub. L. No. 113-283, "Federal Information Security Modernization Act of 2014," December 2014
- OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive 12– Policy for a Common Identification Standard for Federal Employees and Contractors," February 3, 2011
- OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," November 18, 2013
- OMB Memorandum M-15-01, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices," October 3, 2014
- OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996
- DHS Binding Operational Directive 15-01 "Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems," May 21, 2015
- Homeland Security Presidential Directive Number 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

- NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010
- NIST Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011
- NIST Special Publication 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," June 2009
- NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
- NIST Special Publication 800-53A, Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," December 2014
- NASA Policy Directive (NPD) 2800.1B, "Managing Information Technology," March 21, 2008
- NPD 2810.1E, "NASA Information Security Policy," July 14, 2015
- NPD 2830.1A, "NASA Enterprise Architecture," November 2, 2011
- NASA Procedural Requirements (NPR) 2800.1B, "Managing Information Technology," March 20, 2009
- NPR 2810.1A, "Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)," May 16, 2006
- NPR 2830.1A, "NASA Enterprise Architecture Procedures," December 19, 2013
- NASA Handbook ITS-HBK-2810.02-05, "Security Assessment and Authorization: External Information Systems," October 24, 2012

Review of Internal Controls

We evaluated internal controls, including Federal laws, NIST guidance, and NASA policies and procedures and concluded that the internal controls were generally adequate, except in specific circumstances, as discussed in the body of this report. Our recommendation, if implemented, should correct the weaknesses identified.

Prior Coverage

During the last 6 years, the NASA Office of Inspector General and the Government Accountability Office (GAO) have issued 28 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY16 and http://www.gao.gov, respectively.

NASA Office of Inspector General

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)

Federal Information Security Management Act: Fiscal Year 2014 Evaluation (IG-15-004, November 13, 2014)

Audit of the Space Network's Physical and Information Technology Security Risks (IG-14-026, July 22, 2014)

Security of NASA's Publicly Accessible Web Applications (IG-14-023, July 10, 2014)

NASA's Management of its Smartphones, Tablets, and Other Mobile Devices (IG-14-015, February 27, 2014)

Federal Information Security Management Act: Fiscal Year 2013 Evaluation (IG-14-004, November 20, 2013)

NASA's Progress in Adopting Cloud-Computing Technologies (IG-13-021, July 29, 2013)

NASA's Information Technology Governance (IG-13-015, June 5, 2013)

NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools (IG-13-006, March 18, 2013)

Federal Information Security Management Act: Fiscal Year 2012 Evaluation (IG-13-001, October 10, 2012)

Review of NASA's Computer Security Incident Detection and Handling Capability (IG-12-017, August 7, 2012)

NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems (IG-12-006, December 5, 2011)

Federal Information Security Management Act: Fiscal Year 2011 Evaluation (IG-12-002, October 17, 2011)

Inadequate Security Practices Expose Key NASA Network to Cyber Attack (IG-11-017, March 28, 2011)

Preparing for the Space Shuttle Program's Retirement: A Review of NASA's Disposition of Information Technology Equipment (IG-11-009, December 7, 2010)

Federal Information Security Management Act: Fiscal Year 2010 Report from the Office of Inspector General (IG-11-005, November 10, 2010)

Review of NASA's Management and Oversight of Its Information Technology Security Program (IG-10-024, September 16, 2010)

Audit of NASA's Efforts to Continuously Monitor Critical Information Technology Security Controls (IG-10-019, September 14, 2010)

Audit of Cybersecurity Oversight of [a NASA] System (IG-10-018-Redacted, August 5, 2010)

Review of the Information Technology Security of [a NASA Computer Network] (IG-10-013, May 13, 2010)

Government Accountability Office

Information Security: Agencies Need to Improve Cyber Incident Response Practices (GAO-14-354, April 30, 2014)

Information Security: Federal Agencies Need to Enhance Responses to Data Breaches (GAO-14-487T, April 2, 2014)

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent (GAO-14-34, December 9, 2013)

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness (GAO-13-776, September 26, 2013)

Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges (GAO-13-462T, March 7, 2013)

Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards (GAO-11-751, September 20, 2011)

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate (GAO-11-605, June 28, 2011)

Enclosure II: NIST Management Controls

NIST requires agencies to implement information security program management controls to provide a foundation for their information security program. Table 1 provides a list of the management controls.

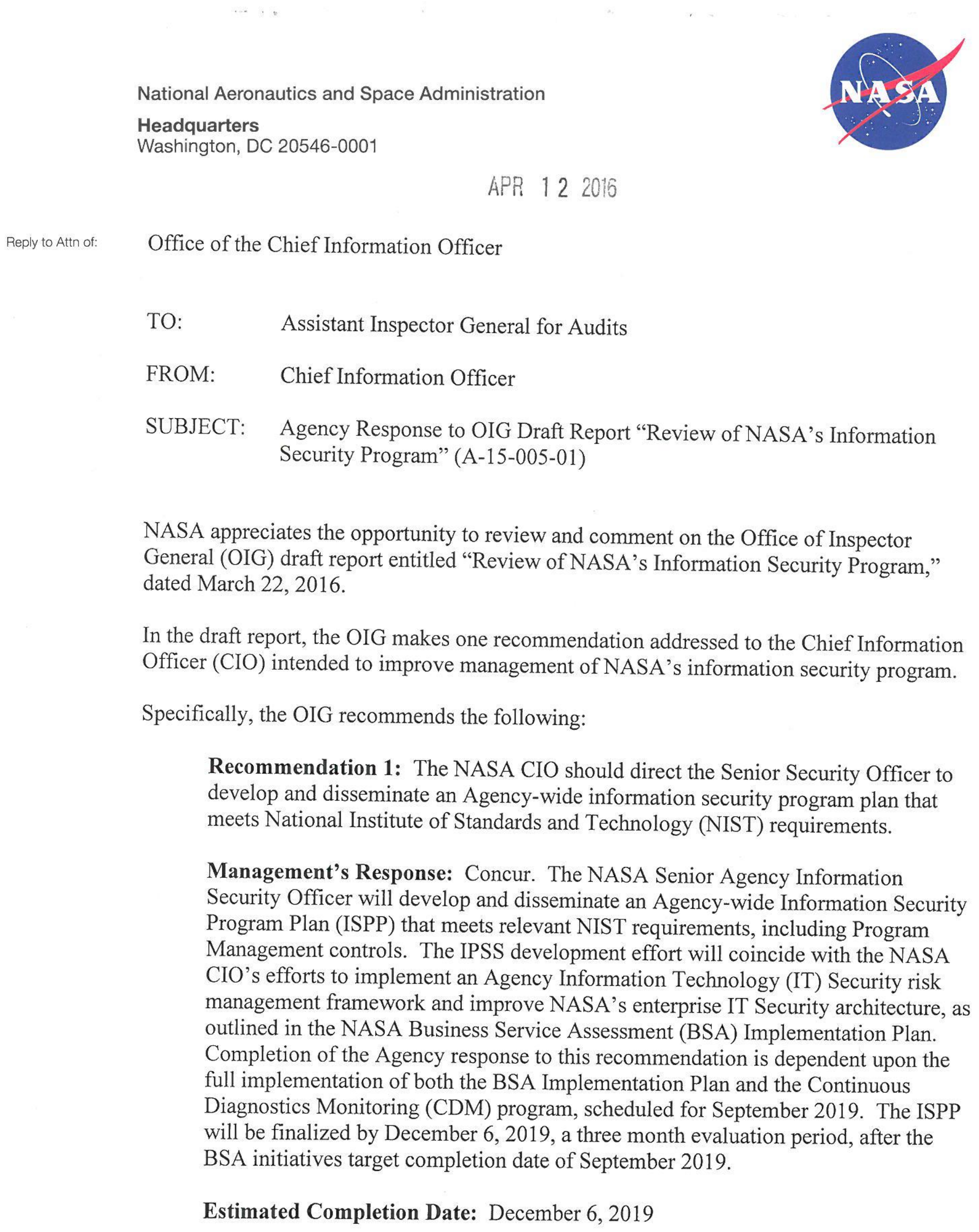
Table 1: Management Controls

Control Number	Management Control
PM-1	Information Security Program Plan
PM-2	Senior Information Security Officer
PM-3	Information Security Resources
PM-4	Plan Of Action And Milestones Process
PM-5	Information System Inventory
PM-6	Information Security Measures Of Performance
PM-7	Enterprise Architecture
PM-8	Critical Infrastructure Plan
PM-9	Risk Management Strategy
PM-10	Security Authorization Process
PM-11	Mission/Business Process Definition
PM-12	Insider Threat Program
PM-13	Information Security Workforce
PM-14	Testing, Training, And Monitoring
PM-15	Contacts With Security Groups And Associations
PM-16	Threat Awareness Program

Source: NIST.

Note: For more information on each management control, visit https://web.nvd.nist.gov/view/800-53/Rev4/family?familyName=PROGRAM%20MANAGEMENT (last accessed March 9, 2016).

Enclosure III: Management Comments



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

APR 12 2016

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 "Review of NASA's Information Security Program" (A-15-005-01)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled "Review of NASA's Information Security Program," dated March 22, 2016.

In the draft report, the OIG makes one recommendation addressed to the Chief Information Officer (CIO) intended to improve management of NASA's information security program.

Specifically, the OIG recommends the following:

> **Recommendation 1:** The NASA CIO should direct the Senior Security Officer to develop and disseminate an Agency-wide information security program plan that meets National Institute of Standards and Technology (NIST) requirements.
>
> **Management's Response:** Concur. The NASA Senior Agency Information Security Officer will develop and disseminate an Agency-wide Information Security Program Plan (ISPP) that meets relevant NIST requirements, including Program Management controls. The IPSS development effort will coincide with the NASA CIO's efforts to implement an Agency Information Technology (IT) Security risk management framework and improve NASA's enterprise IT Security architecture, as outlined in the NASA Business Service Assessment (BSA) Implementation Plan. Completion of the Agency response to this recommendation is dependent upon the full implementation of both the BSA Implementation Plan and the Continuous Diagnostics Monitoring (CDM) program, scheduled for September 2019. The ISPP will be finalized by December 6, 2019, a three month evaluation period, after the BSA initiatives target completion date of September 2019.
>
> **Estimated Completion Date:** December 6, 2019

Enclosure III

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 Ruth McWilliams on (202) 358-5125.

Renee P. Wynn