



## NASA OFFICE OF INSPECTOR GENERAL

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

November 6, 2017

TO: Robert M. Lightfoot Jr.  
Acting Administrator

SUBJECT: Final Memorandum, *Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation* (IG-18-003; A-17-004-00)\*

Dear Acting Administrator Lightfoot,

The NASA Office of Inspector General (OIG) has completed its fiscal year (FY) 2017 summary report evaluating NASA's information security program pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). The law identifies specific security requirements Federal agencies must satisfy and assigns responsibility to agency officials for addressing and Inspectors General for assessing these requirements. For example, agency officials are responsible for developing policies and procedures commensurate with the risk and magnitude of harm from malicious or unintentional impairment of agency information and information systems, while Inspectors General are responsible for performing independent evaluations examining the effectiveness of their agencies' information security program and practices. For this year's review, Inspectors General were required to assess 61 metrics (or questions) in 5 security function areas and test a subset of information systems to determine the maturity of their agency's information security program.

For our FY 2017 review, we assessed NASA's information security policies, procedures, and practices by examining seven information systems. We also assessed the Agency's overall cybersecurity posture using a variety of techniques and leveraged work performed by NASA and other oversight organizations. Finally, we evaluated the Agency's progress in addressing deficiencies identified in prior FISMA and information security reviews. Collectively, those assessments assisted us in reaching our conclusions.

*\*In preparation for public release, selected portions of this report containing sensitive security information have been redacted under exemption (b)(7)(E) of the Freedom of Information Act (FOIA).*

By implementing previous audit recommendations and taking additional corrective actions, NASA is steadily working to improve its overall information security posture. Nevertheless, as indicated by the results of this review, information security remains a significant challenge for NASA and the Agency needs to take considerable action to close cybersecurity capability gaps and combat evolving cyber threats. Moving forward, we will continue to examine NASA's information security program both through focused audits of discrete issues and future FISMA reviews.

We appreciate the courtesies extended to us during this review. If you have questions or wish to comment on the quality or usefulness of this memorandum, please contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or [laurence.b.hawkins@nasa.gov](mailto:laurence.b.hawkins@nasa.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "PKM" followed by a stylized flourish.

Paul K. Martin  
Inspector General

cc: Renee Wynn  
Chief Information Officer

Joseph Mahaley  
Assistant Administrator for Protective Services

Enclosures – 5

*\*In preparation for public release, selected portions of this report containing sensitive security information have been redacted under exemption (b)(7)(E) of the Freedom of Information Act (FOIA).*

## **Enclosure I: Federal Information Security Modernization Act**

The OIG prepared this summary report in response to the FY 2017 reporting requirements for FISMA, which requires the OIG to conduct an annual independent evaluation to determine the effectiveness of NASA's information security program and practices. See Enclosure II for details of the review's scope and methodology.

### **BACKGROUND**

Each day NASA personnel, contractors, academics, and members of the public access NASA's information technology (IT) infrastructure, a complex array of almost 500 information systems geographically dispersed around the world representing an annual investment of approximately \$1.4 billion.<sup>1</sup> This IT infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data.

Like other Federal agencies, NASA's IT infrastructure is under constant attack from domestic and foreign adversaries. Decades of NASA aeronautics and space technology research and development represents hundreds of billions of dollars in U.S. Government and aerospace industry investments. The very nature of NASA's mission, and the valuable technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals, and foreign enterprises. Many of these threats are well-resourced, highly-motivated, and sophisticated.

In December 2014, Congress amended the Federal Information Security Management Act of 2002 and reestablished the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices.<sup>2</sup> The Act also authorizes the Secretary of the Department of Homeland Security (DHS) to implement policies and practices for Federal information systems. OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officers Council, developed the FY 2017 Inspector General (IG) FISMA metrics and reporting requirements to be addressed in OIGs' independent assessments of their agencies' information security programs. These metrics leverage the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and are organized around the Framework's five functions: Identify, Protect, Detect, Respond, and Recover.

---

<sup>1</sup> IT infrastructure refers to the hardware, software, networks, and services required for the operation and management of an enterprise IT environment.

<sup>2</sup> Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

## Cybersecurity Framework

The Cybersecurity Framework provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their enterprise to ensure the effectiveness of security controls over information resources that support Federal operations and assets.<sup>3</sup> This Framework includes activities, desired outcomes, and applicable references common across critical infrastructure sectors and focuses on five specific functions essential to an effective information security program:

1. *Identify*. Develop organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities by identifying and maintaining a hardware and software inventory.
2. *Protect*. Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
3. *Detect*. Develop and implement appropriate activities to identify a cybersecurity event.
4. *Respond*. Develop and implement appropriate activities to take action regarding a detected cybersecurity event.
5. *Recover*. Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity event.

Together, these functions provide a strategic view of the life cycle of an organization's cybersecurity risk management program.

The FY 2017 FISMA metrics are organized around these five functions, with each function tied to one or more of the seven OIG review areas or domains. For example, the Identify function encompasses the risk management domain. Likewise, the Protect function incorporates the configuration management, identity and access management, and security training domains. Table 1 below depicts the alignment of the Cybersecurity Framework functions to the corresponding domains, which are described in detail in the Results section.

**Table 1: Alignment of Cybersecurity Framework with IG FISMA Domains**

Cybersecurity Framework Function	IG FISMA Domains
Identify	Risk Management
Protect	Configuration Management
	Identity and Access Management
	Security Training
Detect	Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: NASA OIG presentation of 2017 FISMA reporting requirements for Inspectors General.

<sup>3</sup> An enterprise is an organization with a defined boundary that uses information systems to execute its mission and manage its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management, human resources, security, information systems, and information and mission management. Security controls are safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

## Reporting Metrics

For FY 2017, DHS, OMB, and CIGIE developed a series of 61 metrics (or questions) to assess the extent to which an agency's information security program complies with FISMA requirements and relevant guidelines. A complete list of these metrics may be accessed at <https://www.dhs.gov/publication/fy17-fisma-documents>. The FY 2017 IG FISMA metrics represent a continuation of work that began in 2015 to align the FISMA evaluation to a maturity model approach that assesses the effectiveness of an entity's information security program based on a 5-level rating system.

1. *Level 1 (Ad-hoc)*. An agency lacks a formalized program and performs activities in a reactive manner.
2. *Level 2 (Defined)*. An agency has a formalized program with comprehensive policies, procedures, and strategies consistent with NIST standards but fails to consistently implement them organization-wide.
3. *Level 3 (Consistently Implemented)*. An agency consistently implements its program but lacks qualitative and quantitative measures and data on its effectiveness.
4. *Level 4 (Managed and Measurable)*. An agency uses metrics to measure and manage implementation of its program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.
5. *Level 5 (Optimized)*. An agency's program is institutionalized, repeatable, self-regenerating, and updated on a near real-time basis based on changes in mission or business requirements and the changing threat and technology landscape.

Ratings throughout the IG FISMA domains are derived by simple majority, where the most frequent level (mode) across the questions serves as that area's rating. For example, if there are seven questions in a domain and an agency receives Level 2 (Defined) ratings for three questions and Level 4 (Managed and Measurable) ratings for four questions, then the domain rating is Level 4 (Managed and Measurable). However, this year OIGs have the discretion to determine the overall rating for each of the five Cybersecurity Framework functions at the maturity level of their choosing based on agency-specific factors such as unique missions, resources, and challenges. Using this approach, OIGs may determine that a particular function area is at a different maturity level than the one produced under a simple majority calculation.

Within the context of the maturity model, OMB designated Level 4 (Managed and Measureable) as an effective level of security. An effective information security program – one that quickly identifies and addresses vulnerabilities – helps ensure continuity of agency operations and reduces the risk that individuals can gain unauthorized access to agency systems and information.

## RESULTS

For our review, we assessed NASA’s information security policies, procedures, and practices by examining seven information systems. We identified these systems from a sample of 496 NASA and contractor information systems provided by the Agency’s Office of the Chief Information Officer (OCIO). We also assessed the Agency’s overall cybersecurity posture using a variety of techniques and leveraged work previously performed by NASA and other oversight organizations. Finally, we evaluated the Agency’s progress in addressing deficiencies identified in prior FISMA and other information security reviews. See Enclosure III for outstanding deficiencies identified in prior OIG FISMA and other IT-related reviews.

Due to the sensitive nature of cybersecurity and related information system vulnerabilities, we have omitted detailed information from this report. Table 2 below summarizes the overall ratings of the Agency’s cybersecurity function areas and the corresponding maturity level for FY 2017. As required, we provided our results to DHS via its web portal.<sup>4</sup>

**Table 2: FY 2017 OIG Assessment of Cybersecurity Function Maturity Level**

Cybersecurity Framework Function	OIG Assessment
Identify	Level 2 – Defined
Protect	Level 2 – Defined
Detect	Level 2 – Defined
Respond	Level 2 – Defined
Recover	Level 2 – Defined

Source: NASA OIG assessment for cybersecurity maturity level rating.

In summary, information security remains a significant challenge for NASA. Although the Agency continues to make progress in implementing cybersecurity initiatives, its cybersecurity program remains ineffective when judged using OMB’s model, which requires agencies to achieve a maturity level of 4 (Managed and Measurable) to be considered effective. In the five function areas, NASA achieved maturity at Level 2 (Defined), indicating the Agency’s information systems remain vulnerable to serious security threats.

That said, NASA has launched multiple initiatives over the past several years to improve its information security program. For example, the Risk Information Security Compliance System (RISCS), Continuous Diagnostics and Monitoring (CDM) program, and the Security Operations Center (SOC) are part of the Agency’s cybersecurity landscape (each of which is described later in the Results section). Once fully implemented, these initiatives should help to address gaps in NASA’s current IT cybersecurity posture and strengthen its risk management strategy. As shown below, Table 3 maps examples of various NASA cybersecurity projects to the corresponding Cybersecurity Framework function.

<sup>4</sup> Our submission to OMB is not contained in this report because OMB designates this information “For Official Use Only.”

**Table 3: NASA Cybersecurity Program Overview**

Cybersecurity Framework Function	Description	NASA Cybersecurity Project
Identify	Develop organizational understanding to manage cyber risk to systems, assets, data, and capabilities by identifying and maintaining a hardware and software inventory	RISCS
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services	Enterprise Internal Border-Network Access Control and Enterprise External Border Protection <sup>a</sup>
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	CDM
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity event	SOC
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cyber event	SOC

Source: NASA OIG representation of data provided by NASA's Office of the Chief Information Officer.

Note: RISCS, CDM, and the SOC are described in further detail in the Results section.

<sup>a</sup> Enterprise Internal Border–Network Access Control enhances the ability to control, identify, and monitor devices connecting to NASA networks. Enterprise External Border Protection creates a network security perimeter to protect against cyber threats.

We describe our findings in each of the five function areas below.

## 1. Identify

The goal of the *Identify* function is to develop the organizational understanding essential to managing cybersecurity risk by identifying and maintaining a hardware and software inventory. By understanding the organization and its mission, the IT resources that support its functions, and related cybersecurity risks, the agency can focus and prioritize its efforts consistent with its risk management strategy and business needs. Based on our review of NASA's efforts in risk management, the Agency is assessed at Level 2 (Defined) for this function. We also considered findings from our previous work in the areas of risk management, cloud computing, IT governance, and other IT security reviews in reaching this conclusion.

### ***Risk Management***

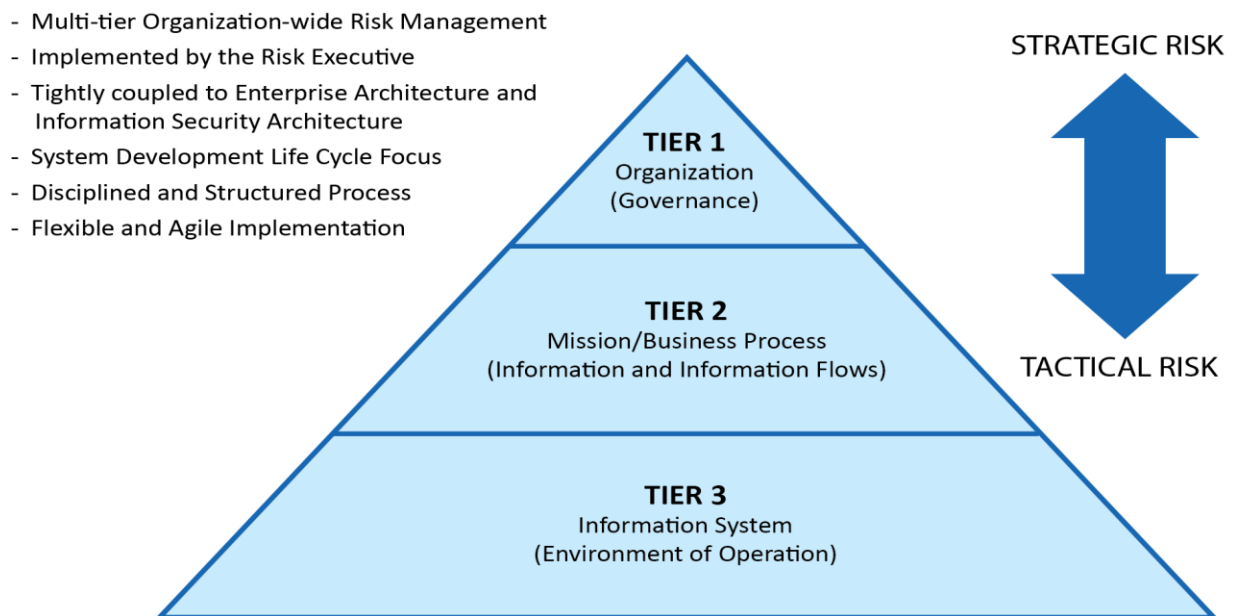
Risk management is a comprehensive process that requires an organization to describe the environment in which risk-based decisions are made to access, respond to, and monitor risk over time. According to NIST, integrating information security requirements and associated security controls into an enterprise's information systems helps ensure security considerations are addressed early in the system's development, and the information security architecture is consistent with the organization's risk

management and information security strategies. Implemented by the Risk Executive, an information security architecture describes how security controls are positioned and how they relate to the overall enterprise architecture (EA).<sup>5</sup>

As Figure 1 below illustrates, a three-tiered approach addresses risk-related concerns such as program and acquisition risk (cost, schedule, and performance), compliance and regulatory risk, financial risk, legal risk, operational risk (mission and business), safety risk, and supply chain risk.

- Tier 1 addresses risk from an organizational perspective, providing the context for all risk management activities carried out by an agency;
- Tier 2 addresses risk from a mission or business process perspective and is driven by the risk context, risk decisions, and risk activities at Tier 1; and
- Tier 3 addresses risk from an information system perspective and is guided by the risk context, risk decisions, and risk activities at Tiers 1 and 2.

**Figure 1: Three-Tiered Approach to Risk Management**



Source: NASA OIG representation of information from NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.

Within risk management, EA is tightly coupled to IT security. EA describes an enterprise's entire set of information systems: how they are configured and integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the mission, and how they contribute to the overall security posture. EA effectiveness is measured using metrics that link successes with the alignment of IT capabilities to mission requirements, improved security, actual cost savings, performance improvements, reduction of duplication, and improved agility and flexibility through simplification and standardization of IT resources. As part of managing risk, FISMA considers

<sup>5</sup> The Risk Executive helps to ensure risk-related considerations for individual information systems, including authorization decisions, are viewed from an organization-wide perspective with regard to overall strategic goals and objectives of the organization. Responsibilities also include ensuring IT security risks are consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission and business success.



whether the agency EA maintains a comprehensive hardware and software inventory, detailed system interconnections, and security integration. NASA's Agency-wide information security architecture is integral to and developed as part of the EA in order to align business, financial, scientific, and engineering needs with its IT infrastructure. EA also directs resources to improve the performance of IT and support Agency missions.

In 2016, as part of the activities related to enterprise risk management, NASA began assigning resources and documenting the information security architecture by transitioning to a centralized toolset – RISCs – to see, track, and report cybersecurity risks. RISCs assigns risk to the appropriate IT System Security Plan, aligns NASA's IT security controls to the Cybersecurity Framework, and reports Agency risk data to Federal dashboards.<sup>6</sup>

The plan of action and milestones (POA&M) process is another important tool used in risk management to track and prioritize potential security problems. NIST requires agencies to develop a POA&M to document and update planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities. NASA established POA&M processes to ensure that IT system weaknesses, control deficiencies, and vulnerabilities identified during security reviews, audits, or other oversight processes are corrected in an efficient and timely manner. The systems we examined utilize the POA&M process to manage risk.

During this review, we found NASA's progress implementing an Agency-wide risk management framework for information security incomplete. While NASA has assigned resources and started to document the Agency's information security architecture, controls related to the Identify function, which include risk management, are insufficient. The Agency does not have automated asset (hardware and software) inventory capabilities and insight into cyber risk for NASA's mission systems.<sup>7</sup> After analyzing the hardware and software inventories, we believe NASA should place greater emphasis on strengthening EA to close the gap between mission systems and inventory and on finalizing transition to and implementation of RISCs to control ongoing cybersecurity risks. By concentrating on information security architecture, NASA can better determine how to effectively invest its resources to ensure security considerations are addressed early in the system development life cycle and that the resulting controls are related to NASA's missions.

Since 2006, the OIG has identified "securing NASA's IT systems and data" as a top management challenge. The OIG has also issued 22 audit reports over the last 5 years containing recommendations to improve NASA's IT security efforts. For example, we have highlighted issues related to cybersecurity vulnerabilities, information security incident detection and handling capabilities, continuous monitoring tools, cloud computing technologies, web application security, and IT governance.

---

<sup>6</sup> Federal dashboards provide a graphical overview of the information needed to manage security controls and maintain awareness of major areas of concern such as vulnerability scan results.

<sup>7</sup> NASA's IT assets generally fall into two broad categories: institutional and mission. Institutional systems support the day-to-day work of NASA employees and include networks, data centers, web services, desktop and laptop computers, enterprise business applications, and other end-user tools such as email and calendaring. Mission systems support the Agency's aeronautics, science, and space exploration programs and host IT systems that control spacecraft, collect and process scientific data, and perform other critical Agency functions.

In addition to our audit work, the Government Accountability Office (GAO) found in a May 2016 audit that NASA security control assessment plans did not include test procedures and that Agency officials had not reviewed or approved in advance the independent assessor's testing procedures.<sup>8</sup> GAO recommended NASA update its security assessment plans to include test procedures and reevaluate security control assessments to ensure they comprehensively test technical controls. NASA's Chief Information Officer concurred with GAO's recommendations and noted actions the Agency would take, including implementation of a commercial assessment tool, as well as expected time frames for their completion (currently FY 2018).

In sum, while NASA has established a risk management program with policies and procedures consistent with NIST requirements, the program lacks an integrated Agency-wide risk management strategy and a comprehensive approach towards information security, including an IT asset inventory capability that integrates fully into the broader enterprise risk management process.

## 2. Protect

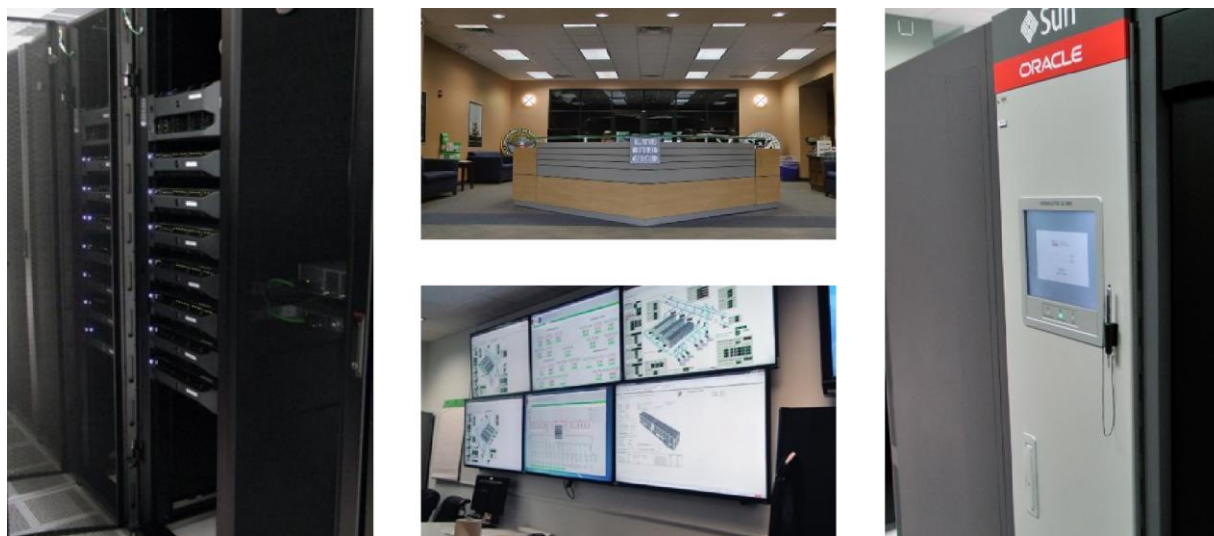
The goal of the *Protect* function is to ensure that agencies safeguard their systems, networks, and facilities with appropriate cybersecurity defenses. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the domains of configuration management, identity and access management, and security training. Based on our review of NASA's efforts in those areas, the Agency is assessed at Level 2 (Defined). We also considered findings from our previous work in the areas of IT configuration management, identity and access management, external network connectivity, and other IT security reviews in reaching our conclusion.

### *Configuration Management*

The configuration of an information system and its components has a direct impact on its security posture. Proper configuration management requires an ongoing investment of time and resources to address product patches, fixes, and updates. As changes to information systems are made, baseline configurations are updated; specific configuration settings are confirmed; and configuration items are tracked, verified, and reported. The challenge is not only to establish an initial baseline configuration that represents a secure state – while being cost-effective, functional, and supportive of mission and business processes – but also to maintain a secure configuration given the continually evolving nature of information systems and the missions they support. Figure 2 depicts diverse examples of information systems used by NASA, which includes (clockwise from left) a collection of computer servers, a credential and security verification reception area, backup tape library system, and an operations control center. The operations control center monitors each of the information systems to ensure protection and management of the IT infrastructure.

---

<sup>8</sup> GAO, "Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems" (GAO-16-501, May 18, 2016). Security control assessment is the testing and evaluation of the management, operational, and technical security controls in an information system to determine 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 system.

**Figure 2: Examples of NASA Information Systems**

Source: NASA OIG representation of NASA information systems.

When establishing baseline configurations, NASA consults a variety of sources including NIST guidance, Center for Internet Security (CIS) benchmarks, and industry best practices.<sup>9</sup> In 2005, NASA began establishing “baselines” to ensure infrastructure compliance with security configuration guidelines. The establishment of security baselines is an ongoing process and some necessary baselines are not yet in place. In cases where a NASA security baseline does not currently exist, the Agency instead adopts CIS benchmarks. For information systems and applications not covered by NASA security baselines or CIS benchmarks, the Agency may obtain baseline configurations from other Government and commercial sources such as the Defense Information Security Agency or Microsoft Corporation. Where no appropriate third-party sources are available, Center IT specialists develop their own baseline configurations.

More broadly, NASA continues to struggle with implementing secure configuration settings in an environment with diverse operating systems and applications.<sup>10</sup> For example, during this year’s review the compliance rate with NASA security baselines averaged 79 percent for Windows devices. However, for Windows servers – considered a higher risk because they provide services to other computer devices over a network – the compliance rate for implementation of secure configuration settings dropped to 49 percent. Although NASA is working toward eliminating unsupported operating systems such as Windows XP and Windows Server 2003, configuration management remains a serious life cycle concern.

In sum, although NASA has established a configuration management program, it still needs to fully implement secure configuration settings, improve hardware and software asset management, and remediate configuration-related vulnerabilities such as unsupported operating systems.

<sup>9</sup> CIS is a non-profit entity that establishes benchmarks, which are the global standard and recognized best practices for securing IT systems and data against cyberattacks.

<sup>10</sup> Operating systems (OS) consist of software that manages the memory, processes, and hardware of a computer system. Through their life cycle, OS require vendor support in the form of upgrades, fixes, and new versions. An OS life cycle begins upon its release and concludes when vendor support ends. Vendors publish end-of-support dates on their websites to inform the public when their OS support will terminate. For example, Microsoft Corporation stopped providing security updates and technical support for Windows XP in April 2014 and Windows Server 2003 in July 2015.

## *Identity and Access Management*

A key goal of identity and access management is to ensure access rights to an agency's IT systems are provided only to authorized individuals. Homeland Security Presidential Directive-12 (HSPD-12) is a 2004 Federal identity management initiative that seeks to provide secure and reliable forms of identification for Government employees and contractors.<sup>11</sup> HSPD-12 requires agencies, to the maximum extent practicable, to follow specific technical standards and business processes when issuing Federal Personal Identity Verification (PIV) credentials, including standard background investigations to verify the identities of employees and contractors.<sup>12</sup>

In February 2011, OMB issued Memorandum M-11-11 requiring Federal agencies to develop an implementation policy to use PIV credentials as a primary source for physical access to Federal facilities and for logical access (passwords or biometrics) to Federal information systems.<sup>13</sup> Further, a DHS attachment to OMB M-11-11 states that since FY 2012, agencies' implementation policies must require the upgrade of existing physical access control systems to use PIV credentials and the ability to accept and electronically verify PIV credentials issued by other Federal agencies.

NASA's OCIO and the Office of Protective Services jointly manage the Agency's Identity, Credential, and Access Management (ICAM) program to meet the requirements of HSPD-12 and OMB M-11-11. The ICAM program consists of three parts: identity management, credential management, and access management.

1. *Identity management* includes basic details about an individual such as their affiliation with NASA, position risk and sensitivity, and information about the individual's background investigation. This information is used to determine what IT systems an individual may access.
2. *Credential management* identifies what media (hard or soft) may be used to permit access. Credentials include badges, user identification, password, and tokens.
3. *Access management* provides permissions and controls to ensure that only authorized persons gain access to NASA assets. This includes the request, approval, and provisioning of access to NASA's physical assets (facilities) and information systems (computer applications and data).

NASA's ICAM program also includes a concept known as "federation," which allows NASA to trust external partners to perform some PIV management services for individuals who are not associated with NASA but require access to Agency assets. For example, a visitor from another Federal agency may present his or her PIV smartcard for identification purposes at a NASA Center. In addition, off-site NASA contractors may use company-issued, Federally-approved smartcards to access NASA systems to which they are authorized.

---

<sup>11</sup> HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

<sup>12</sup> A PIV card is an identity or "smart" card issued to an individual that contains identity credentials such as a photograph, cryptographic keys, or digitized fingerprint representation so the identity of the cardholder can be verified. Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed, such as low-risk, public-facing websites.

<sup>13</sup> OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," February 3, 2011.

In June 2015, as part of a security review known as the 30-day Cybersecurity Sprint, OMB required Federal agencies to tighten access for privileged users and increase the use of multi-factor authentication.<sup>14</sup> This exercise, a response to the massive breach in Office of Personnel Management information systems, required all Federal agencies to take immediate action to improve the security of their information systems and data. Consequently, NASA acquired a tool to enhance its use of PIV credentials and allow privileged users to access Agency systems using PIV authentication. In 2016, NASA achieved 100 percent PIV authentication for its privileged users. Moreover, in FY 2017 NASA increased the use of PIV authentication for its unprivileged users from 54 percent to 65 percent. By December 2017, NASA expects to increase the use of PIV authentication by another 15 percent through implementation of a similar solution for Apple computers. Previously, PIV implementation was only available to Windows computers.

We found appropriate identity and access controls were in place for each of the seven information systems reviewed. NASA generally uses the electronic capabilities of the PIV credentials for authentication to Agency systems and networks. Nevertheless, although NASA has implemented a variety of access management controls, including PIV authentication, firewalls, and routers to enable secure access to the Agency's information systems, the Agency needs to focus on increasing the use of PIV authentication for unprivileged users to enhance its broader security strategy.<sup>15</sup>

In sum, the NASA identity and access management program has made progress with respect to the implementation of PIV credentials as the primary means for logical access to its information systems, but more work remains to implement PIV for unprivileged users.

### *Security Training*

Consistent with Federal guidance, NASA requires all users to complete annual online security awareness training available on the Agency's training website. Users with significant information security responsibilities or elevated access to NASA information must complete additional security training appropriate to their roles, including operating system security and IT security for administrators.<sup>16</sup>

Located at Glenn Research Center, the IT Security Awareness and Training Center (ITSATC) is responsible for increasing the information security awareness and knowledge of the NASA workforce. According to ITSATC, its objectives are to (1) equip NASA employees with necessary tools and knowledge to be effective in the application of policies, standards, and procedures; (2) enhance end-user knowledge of cyber threats and vulnerabilities within the NASA environment through role-based training; (3) provide training opportunities to assist employees in developing the necessary skills to recognize, assess, and mitigate cyber threats and vulnerabilities; and (4) provide outreach to IT and Security Specialists focusing on issues of interest to NASA users and current information security challenges.

---

<sup>14</sup> A privileged user is someone authorized to perform security-relevant functions that other users are not authorized to perform. Multi-factor authentication requires verifying the identity of a user using two or more factors as a prerequisite to IT system access. Authentication factors include something you know (password, Personal Identification Number), something you have (PIV identification device, token), or something you are (biometric finger print).

<sup>15</sup> A firewall is a hardware and software capability that limits access between networks and/or systems in accordance with a specific security policy. Routers are small electronic devices that join multiple computer networks together via either wired or wireless connections.

<sup>16</sup> Significant information security responsibilities include users with privileged network user accounts; users who have managerial, administrative, or operational responsibilities that enable them to affect system or information security; and senior officials such as Chief Information Officers and Center Chief Information Security Officers.

The training center offers courses and webinars on IT topics such as Cybersecurity, Anti-Phishing, Role-Based System Administration, Social Networking, Malware, Mobile Device Security, and Identity Theft.<sup>17</sup> Additionally, ITSATC distributes a quarterly newsletter with IT security information sections titled *Internet Safety*, *Insider Threats*, and *When Data Exposure Becomes a Breach*.

The NASA OCIO regularly conducts social engineering exercises such as phishing to test its ability to gain unauthorized access to NASA information and systems. These exercises are part of two separate cybersecurity operations projects conducted across the Agency:

1. The OCIO performs annual penetration testing that includes social engineering exercises at each NASA Center and facility.
2. The OCIO conducts quarterly phishing exercises that target large segments of the NASA general IT user population to assess the effectiveness of social engineering training and phishing email awareness integration into NASA IT Security Awareness training.

During the second quarter of 2017, NASA conducted a phishing exercise using a new highly sophisticated, single-scenario email that mimicked legitimate communications. Due to the new style of testing, [REDACTED]

(b)(7)(E)

[REDACTED] Fortunately, almost double the number of people compared to the last test reported the email to the SOC, NASA's nerve center for detection and monitoring of security incidents for the Agency. [REDACTED]

(b)(7)(E)

[REDACTED] Although NASA incorporates phishing awareness as part of its annual security awareness training, we consider (b)(7)(E) [REDACTED] and encourage that separate, revised phishing security awareness training be conducted annually. By highlighting and segregating phishing-threat education, non-expert users will achieve a better level of awareness and be less susceptible to threats that cause harm to NASA systems or expose Agency data and IT infrastructure. Effective August 1, 2017, the OCIO and Office of Human Capital Management required supplemental phishing awareness training for NASA IT users who click on the link.

Further, an increased emphasis on role-based training is underway in response to a 2016 GAO audit.<sup>18</sup> Robust security awareness and an associated training program is critical to ensuring that employees understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them. While broad-based awareness initiatives provide the rules of good security practices to the workforce, high trust and high impact positions such as IT security program managers, security officers, and system administrators require role-based training. Role-based training provides individuals the information required to perform the IT security responsibilities specific to their role at the Agency based on their knowledge, skills, and abilities. To this end, NASA has defined role-based training requirements and implemented this training for personnel with significant security responsibilities. In July 2017, GAO closed out the recommendation from its 2016 audit regarding role-based training.

<sup>17</sup> Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual and attempt to entice users to click on a link that will take them to a fraudulent website that also appears legitimate. Malware is a program inserted into a computer with the intent of compromising the operating system, applications, or data.

<sup>18</sup> GAO-16-501.



In sum, although NASA is maintaining an information security training program consistent with NIST requirements, the Agency needs to ensure completion of applicable role-based training for personnel with significant security responsibilities. Additionally, to improve the overall rating for the Protect function, the Agency needs to improve security controls for identity and access management as well as configuration management.

### 3. Detect

The *Detect* function enables timely discovery of cybersecurity events and encompasses continuous monitoring activities. Based on our review of NASA's efforts in continuous monitoring, the Agency is assessed at Level 2 (Defined). We also considered findings from our previous work in the areas of vulnerability monitoring, mobile devices, and other IT security reviews in reaching our conclusion.

#### *Continuous Monitoring*

Continuous monitoring of security controls is an essential element of NASA's information security program and is used to determine whether an information system's key security controls are effective over time in light of changes to system hardware and software. A well-designed and well-managed continuous monitoring program can transform an otherwise static and fixed security control assessment and risk determination process into a real-time process that provides essential information about a system's security status. This in turn enables NASA officials to take timely risk mitigation actions and make risk-based decisions regarding the operation of Agency information systems.

The concept of monitoring information system security has long been recognized as a sound management practice. In 1996, OMB Circular A-130 required agencies to review information systems' security controls and ensure system changes did not have a significant impact on security, security plans remained effective, and security controls continued to perform as intended.<sup>19</sup> FISMA further emphasized the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency appropriate to the system's risk, but not less than annually.

In 2011, NIST provided guidelines for agencies to develop and implement an information security continuous monitoring strategy and program, which is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.<sup>20</sup> Any effort or process intended to support ongoing monitoring of information security across an organization begins with leadership defining a comprehensive continuous monitoring strategy encompassing technology, processes, procedures, operating environments, and people.<sup>21</sup> The strategy should

- instill a clear understanding of organizational risk tolerance, set priorities, and manage risk;
- include metrics that provide meaningful indications of security status at all organizational tiers;

<sup>19</sup> OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996. The current version of this Circular dated July 28, 2016, is titled, "Managing Federal Information as a Strategic Resource."

<sup>20</sup> Ongoing monitoring, a critical part of an agency's Risk Management Framework, is a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

<sup>21</sup> NIST named the individual who oversees an organization's continuous monitoring strategy and program as the Risk Executive.

- ensure continued effectiveness of all security controls;
- ensure compliance with information security requirements derived from organizational missions or functions, Federal legislation, directives, regulations, policies, standards, and guidelines;
- include all organizational information assets and help maintain visibility into asset security;
- ensure knowledge and control of changes to organizational systems and environments of operation; and
- maintain awareness of threats and vulnerabilities.

Subsequently, DHS, in partnership with the General Services Administration, established a Government-wide acquisition vehicle for a Continuous Diagnostics and Mitigation (CDM) program to identify security issues and help meet Federal security requirements. Led by DHS, the CDM program provides agency system and network administrators the capabilities and commercial off-the-shelf tools to know who and what is connected to their networks, current vulnerabilities, configuration management, and event detection and response. To address gaps in cybersecurity, Government-wide CDM implementation is structured in three phases: (1) endpoint integrity (devices), (2) infrastructure integrity (people), and (3) boundary protections (events).<sup>22</sup> In September 2015, DHS awarded a task order to Booz Allen Hamilton to implement CDM services at NASA and several other agencies. In 2016, NASA began working with Booz Allen to identify the monitoring technologies needed for asset management and to integrate the necessary IT security tools and services into NASA's enterprise. During 2017, NASA continued to make progress towards CDM phase 1 implementation with anticipated completion in FY 2018.

As shown in Figure 3, CDM works to provide continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, and prioritizing risk alerts.<sup>23</sup> First, agency-installed sensors perform an automated search for known cyber flaws. Next, results are collected, analyzed, and fed into a dashboard that produces customized reports, alerting network managers to fix their most critical cyber risks. Prioritized alerts enable agencies to efficiently allocate resources based on the severity of the risk. Finally, progress reports track results and feed summary information into the dashboard to provide situational awareness into cybersecurity risk posture. CDM is designed to scan all agency IT systems at least once every 72 hours.

---

<sup>22</sup> Endpoint integrity focuses on hardware and software asset management, configuration settings, known vulnerabilities, and malware; infrastructure integrity focuses on account and privilege management, configuration settings, ports, protocols, and services; and boundary protections focus on event detection and response, encryption, remote access, and access control.

<sup>23</sup> The term "sensor" is used broadly to define anything that senses, queries, contains, or provides data to CDM. Sensors identify risks or gaps in the agency's network protection or collect data from department and agency networks in order to identify unusual or irregular network activity, such as an unsanctioned device being installed on an agency network or an adversary trying to copy data.



---

**Figure 3: Continuous Diagnostics and Mitigation Process**



---

Source: U.S. Department of Homeland Security.

We found that integrating continuous monitoring activities across NASA's enterprise infrastructure is immature due, in part, to an incomplete automatic hardware and software inventory sensor detection capability. While the early phases of CDM is providing insight into the Agency's institutional IT environment, NASA currently lacks inventory sensor detection capability for the mission systems that support its aeronautics, science, and space exploration programs. As a result, NASA's inventory remains incomplete and at risk in the broader enterprise risk management process. Further, the Agency lacks an enterprise Data Loss Prevention capability including the ability to test, detect, and investigate data exfiltration attempts.<sup>24</sup> Without an accurate inventory of all systems, NASA cannot ensure it is applying appropriate security controls, nor can it verify all security controls that protect agency IT systems are effective.

In sum, while NASA has established an enterprise-wide continuous monitoring program consistent with NIST requirements, the Agency needs to improve its program by developing a comprehensive continuous monitoring strategy for automatic hardware and software inventory detection and data exfiltration defense capabilities.

## 4. Respond

The *Respond* function ensures that agencies have policies and procedures in place that detail how they will respond to cybersecurity events, with a focus on incident response testing and communications. Based on our review of NASA's efforts in incident response, the Agency is assessed at Level 2 (Defined). We also considered findings from our previous work in the areas of cybersecurity incident response and handling and other IT security reviews in reaching our conclusion.

---

<sup>24</sup> Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server, usually performed by cyber criminals over the Internet or other network.

## *Incident Response*

An information security incident is an adverse event or situation that poses a threat to the integrity, availability, or confidentiality of an organization's information systems or data. NASA's incident response and reporting program seeks to provide timely identification, response, and resolution of security incidents.

In November 2008, NASA consolidated its Center-based computer security incident detection and response programs into the SOC in an effort to improve its capability to detect and respond to evolving threats posed by increasingly sophisticated cyberattacks. Located at Ames Research Center, the SOC provides an Agency-wide single point-of-contact for information security incidents and continuously monitors computer network traffic entering and leaving NASA Centers. The SOC also maintains the Incident Management System, a database used to coordinate, track, and report information about security incidents. In the first three quarters of FY 2017, 989 security incidents were reported to the SOC: 317 in the first quarter, 348 in the second, and 324 in the third, with the increase in the number of incidents in the second quarter attributable to an increase in attackers' use of malware. Examples of cybersecurity incidents that affected agencies and other entities include:

- An incident in which users are tricked into opening a "quarterly report" sent via email that is actually malware, resulting in the tool infecting their computers and establishing connections with an external host.
- An incident where an attacker obtains sensitive data and threatens to publicly release the details if the organization does not pay a designated sum of money.
- An incident where a user provides illegal copies of software to others through file-sharing services.

FISMA requires Federal agencies to report such incidents to the U.S. Computer Emergency Readiness Team (US-CERT), a Government-wide incident response organization under DHS that assists Federal civilian agencies in their incident handling efforts. US-CERT does not replace existing agency response teams; rather, it augments the efforts of Federal civilian agencies by serving as a focal point.

(b)(7)(E)

[REDACTED]

<sup>25</sup> (b)(7)(E)

[REDACTED] To further examine SOC operations, the OIG has an ongoing audit that is evaluating its capability, workload, resource management, and continuity of its incident response capabilities.<sup>26</sup>

<sup>25</sup> NASA OIG, "Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 7, 2012).

<sup>26</sup> NASA OIG, "Audit of NASA's Security Operations Center" (A-17-009-00). This report is estimated to be issued by the end of 2017.

In sum, while NASA is maintaining an incident response and reporting program consistent with NIST requirements, the program needs to ensure sufficient incident monitoring and detection coverage is available in the event of a SOC disruption. Further, the Agency must evolve from the reactive analysis of cyber threat alerts to proactive strategic intelligence gathering necessary to defend its information systems.

## 5. Recover

The *Recover* function supports timely recovery to normal operations to reduce the impact from a cybersecurity event by focusing on contingency planning. Based on our review of NASA's efforts in contingency planning, the Agency is assessed at Level 2 (Defined). We also considered findings from our previous work in the areas of contingency planning, the SOC, and other IT security reviews in reaching our conclusion.

### *Contingency Planning*

Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient interim solutions to enhance system availability. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

We examined NASA's contingency planning controls such as testing and back-up capacity for the seven selected information systems and found appropriate controls in place. While the Agency is maintaining business continuity and disaster recovery plans consistent with NIST requirements, [REDACTED]

(b)(7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## CONCLUSION

Despite progress made to address previously identified weaknesses related to its cybersecurity program, we concluded that NASA, based on the results of our current review, has not implemented an effective information technology security program. Further, without implementing additional improvements to ensure that NIST requirements are implemented, the Agency may lose ground in its efforts to address the challenges in a rapidly evolving cybersecurity landscape. To strengthen its information security program, we believe the Agency should continue its initiatives in each of the seven IG FISMA domains.

1. *Risk Management.* Strengthen the enterprise architecture risk management framework by closing the gap between mission systems and inventory, and complete the transition to RISCS.
2. *Configuration Management.* Augment secure configuration settings, improve hardware and software asset management, and remediate configuration-related vulnerabilities including unsupported operating systems.
3. *Identity and Access Management.* Increase the use of PIV authentication for unprivileged users.
4. *Security Training.* Complete applicable role-based training for personnel with significant security responsibilities.
5. *Continuous Monitoring.* Develop a comprehensive continuous monitoring strategy for automatic hardware and software inventory detection and data exfiltration defense capabilities.
6. *Incident Response.* Bridge the gap between reactive and proactive intelligence gathering and analysis techniques.
7. *Contingency Planning.* (b)(7)(E) .

Finally, we are concerned that many recommended corrective actions from prior FISMA and other IT-related reviews remain open after more than a year. We urge a renewed Agency commitment to addressing our previous recommendations given the constant and growing cybersecurity threats. Although this memorandum made no specific recommendations to NASA, management provided a brief response that is reproduced in Enclosure V. Technical comments provided by management have been incorporated, as appropriate.

---

Major contributors to this memorandum include Mark Jenson, Financial Management Director; Mindy Vuong, Project Manager; Wayne Emberton; Linda Hargrove; and Lynette Westfall. Lauren Suls provided editorial and graphic assistance.

## **Enclosure II: Scope and Methodology**

We performed this review from January through October 2017 in accordance with the Quality Standards for Inspection and Evaluation issued by CIGIE. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

To conduct our review, we evaluated the effectiveness of NASA's information security program and practices. Specifically, we (1) designed a comprehensive evaluation approach to identify deficiencies utilizing FISMA's five function areas of the Cybersecurity Framework; (2) used last year's FISMA evaluation as a baseline for this year's evaluation; (3) reviewed applicable laws, regulations, policies, and guidance; (4) interviewed NASA security officials and staff at Headquarters and selected NASA Centers; (5) assessed the status of RISCs; (6) reviewed and analyzed information system documentation including security plans, risk assessments, security scans, accreditation, training, POA&Ms, and SOC incidents; (7) determined whether deficiencies identified in previous FISMA reviews continued to exist; and (8) analyzed the impact of recently completed or ongoing NASA reviews, OIG audits, and other oversight organization assessments. We did not evaluate the technical adequacy of the documents other than to determine whether they generally met OMB and NIST guidelines.

### ***Federal Laws, Regulations, Policies, and Guidance***

To accomplish our objective, we reviewed and evaluated relevant:

- Federal laws and regulations pertaining to IT and cybersecurity;
- OMB guidance and annual reporting instructions for FISMA;
- DHS FISMA metrics for 2017;
- CIGIE and Federal Chief Information Officers Council IT guidance;
- Security controls and best-practices issued by NIST for the planning and management of IT systems and information security; and
- NASA policy directives, procedural requirements, and IT security handbooks.

### **Sampling**

For this review, we used a judgmental sampling method based on Authorization to Operate expiration dates, POA&M due dates, and Center locations. Staffing limitations prevented the use of statistical sampling. To identify the population of systems, we obtained the 2017 inventory of NASA and contractor information systems from the NASA OCIO and removed systems reviewed during previous FISMA reviews, as well as OIG systems.

We determined that a representative sample of seven systems would be reviewed – three systems at Kennedy Space Center, two systems at Goddard Space Flight Center, and two systems at Stennis Space Center.

## Use of Computer-Processed Data

We used limited computer-processed data to perform this review. Specifically, we analyzed data and security scan results from NASA's IT inventory system as provided by the OCIO or Center officials. Although we did not independently verify the reliability of this information, we compared it with other available supporting documents to determine data consistency and reasonableness. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

## Review of Internal Controls

We reviewed and evaluated internal controls related to NASA's management of its information security program, as well as those related to our sample of seven information systems. We examined controls as they relate to the five FISMA function areas of the Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. As discussed in this report, we found that internal controls in some areas need improvement.

## Prior Coverage

During the last 5 years, the NASA OIG and GAO have issued 30 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at <https://oig.nasa.gov/audits/reports/FY18/index.html> and <http://www.gao.gov>, respectively.

### *NASA Office of Inspector General*

*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)

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

*NASA's Management of the Near Earth Network* (IG-16-014, March 17, 2016)

*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 Compliance with Executive Order 13526: Classified National Security Information* (IG-13-023, September 26, 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)

### ***Government Accountability Office***

*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)

*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)



## Enclosure III: Outstanding Deficiencies Identified in Prior OIG FISMA and Other IT-Related Reviews

This enclosure summarizes, by audit, the status of outstanding deficiencies identified in prior FISMA and other IT-related reviews. As noted in the table below, many corrective actions are not due to be completed until 2018 or 2019.

**Table 4: Outstanding FISMA-Related Deficiencies by Audit**

Metrics	OIG Report Title, Number, and Date Issued	Outstanding Deficiency Description	Latest Target Corrective Action Completion Date
<ul style="list-style-type: none"> <li>• Protect</li> <li>• Detect</li> <li>• Respond</li> <li>• Recover</li> </ul>	Review of NASA's Computer Security Incident Detection and Handling Capability (IG-12-017, August 7, 2012)	(b)(7)(E)	May 2018
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> <li>• Detect</li> </ul>	NASA's Management of its Smartphones, Tablets, and Other Mobile Devices (IG-14-015, February 27, 2014)	We found the Agency needs to implement a tool to mitigate risks when smartphones and tablets connect to NASA systems other than email.	January 2019
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> <li>• Detect</li> </ul>	Security of NASA's Publicly Accessible Web Applications (IG-14-023, July 10, 2014)	We noted deficiencies in the design and implementation of NASA's Web Application Security Program that left the Agency's publicly accessible web applications at risk of compromise.	December 2017
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> <li>• Detect</li> </ul>	Audit of the Space Network's Physical and Information Technology Security Risks (IG-14-026, July 22, 2014)	We highlighted deficiencies with risk assessment controls and vulnerability scanning on certain wide-area network infrastructure associated with the Space Network and White Sands Test Facility.	April 2018
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	NASA's Management of the Deep Space Network (IG-15-013, March 26, 2015)	We found NASA failed to follow established Agency policies, standards, and governance methodologies for the security of the Deep Space Network's IT and physical infrastructure.	November 2018
<ul style="list-style-type: none"> <li>• Protect</li> <li>• Detect</li> </ul>	NASA's Management of the Near Earth Network (IG-16-014, March 17, 2016)	We found components of the Near Earth Network did not have properly applied or monitored security configuration baselines, which left the Network less secure, more prone to compromise, and lacking useful information to respond to a cyberattack.	March 2018
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> <li>• Detect</li> </ul>	Review of NASA's Information Security Program (IG-16-016, April 14, 2016)	We reported the Agency needed to enhance its efforts in three IG FISMA domains: continuous monitoring, configuration management, and risk management.	December 2019

<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	<p>Security of NASA's Cloud Computing Services (IG-17-010, February 7, 2017)</p>	<p>We found continuing weaknesses in NASA's governance and risk management processes have prevented the Agency from fully realizing the benefits of cloud computing and continue to leave Agency information stored in cloud environments at unnecessary risk.</p>	<p>January 2019</p>
<ul style="list-style-type: none"> <li>• Identify</li> <li>• Protect</li> </ul>	<p>Industrial Control System Security within NASA's Critical and Supporting Infrastructure (IG-17-011, February 8, 2017)</p>	<p>We found NASA has not adequately defined operational technology, developed a centralized industrial control inventory, or established a standard protocol to protect systems that contain operational technology components, which can cause the underlying systems to malfunction. Further, NASA's policies do not distinguish operational technology from IT, and the Agency does not offer training focused on protecting operational technology systems.</p>	<p>October 2018</p>

Source: NASA OIG.

## Enclosure IV: Glossary

This enclosure is a glossary of terms used throughout our FISMA review and corresponding definitions.

**Dashboard.** A graphical overview, or summary, of the information needed to manage security controls and maintain awareness of major network areas of concern.

**Data Exfiltration.** The unauthorized copying, transfer, or retrieval of data from a computer or server, usually performed by cyber criminals over the Internet or other network.

**Domain.** An environment that includes a set of system entities that have the right to access computer resources defined by a common security policy, security model, or security architecture. Examples of domains include risk management, configuration management, identification and access management, security training, continuous monitoring, incident response, and contingency planning.

**Enterprise.** An organization with a defined boundary that uses information systems to execute its mission and manages its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management, human resources, security, information systems, and information and mission management.

**Firewall.** A hardware and software capability that limits access between networks and/or systems in accordance with a specific security policy.

**Information Security.** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

**Information System.** A system made up of hardware, software, data, people, and a process, and refers to a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**Information Technology Infrastructure.** The hardware, software, networks, and services required for the operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners, and customers.

**Malware.** A program that is inserted into a computer with the intent of compromising the operating system, applications, and/or data.

**Multi-factor Authentication.** Verifying the identity of a user using two or more factors as a prerequisite to IT system access. Authentication factors include something you know (password, Personal Identification Number), something you have (cryptographic identification device, token), or something you are (biometric finger print).

**Operating System.** Software that manages the memory, processes, and hardware of a computer system.

**Personal Identity Verification.** An identity or “smart” card issued to an individual that contains identity credentials such as a photograph, cryptographic keys, or digitized fingerprint representation so the identity of the cardholder can be verified.

**Phishing.** An attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual and attempt to entice users to click on a link that will take them to a fraudulent website that also appears legitimate.

**Privileged User.** A user that is authorized and trusted to perform security-relevant functions that other users are not authorized to perform.

**Router.** A small electronic device that joins multiple computer networks together via either wired or wireless connections.

**Security Control Assessment.** The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine 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 system.

**Security Controls.** The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

**Sensor.** A broad term used to define anything that senses, queries, contains, or provides data to CDM. Sensors identify risks or gaps in the agency's network protection or collect data from department and agency networks in order to identify unusual or irregular network activity, such as an unsanctioned device being installed on an agency network or an adversary trying to copy agency data from the agency's network.

**Significant Security Responsibilities.** Users with privileged network user accounts; users who have managerial, administrative, or operational responsibilities that enable them to affect system or information security; and senior officials such as Chief Information Officers and Center Chief Information Security Officers.

## Enclosure V: Management Comments

National Aeronautics and Space Administration  
**Headquarters**  
Washington, DC 20546-001



OCT 31 2017

Reply to Attn of:

Office of the Chief Information Officer

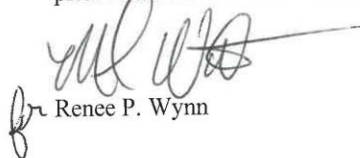
TO: Assistant Inspector General for Audits  
FROM: Chief Information Officer  
SUBJECT: Agency Response to OIG Draft Report, "Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation" (A-17-004-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General draft report entitled, "Federal Information Security Modernization Act (FISMA) Fiscal Year 2017 Evaluation" (A-17-004-00), dated October 18, 2017.

While the report contains no specific recommendations to NASA, it does highlight issues and challenges in each of the seven Inspector General (IG) FISMA domains. NASA is committed to continuing our initiatives in each of these domains to strengthen our cybersecurity program. For example, NASA continues to implement the "Personal Identity Verification (PIV)-Mandatory" project to enforce PIV card authentication for NASA information technology (IT) and unprivileged network accounts across the Agency – a critical effort to verify and secure our IT assets, networks, and people. We are also continuing to deploy the Department of Homeland Security's Continuous Diagnostics and Mitigation Program tools and sensors on NASA's networks and IT assets, enabling improved security monitoring and cybersecurity risk mitigation capabilities.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, though not classified, we have identified information that should not be publicly released in its entirety and recommend that it be considered Sensitive But Unclassified.

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