NASA OFFICE OF INSPECTOR GENERAL

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

November 7, 2016

TO: Charles F. Bolden, Jr.
Administrator

SUBJECT: Final Memorandum, *Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation* (IG-17-002; A-16-009-00)*

Dear Administrator Bolden,

The NASA Office of Inspector General (OIG) has completed its fiscal year (FY) 2016 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.

FISMA requires the OIG tests a representative subset of NASA's systems. For our FY 2016 review, we used a risk-based approach to examine a sample of five Agency and contractor information systems. We also considered findings from our previous work in reaching our conclusions.

By implementing previous audit recommendations and taking additional 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 top management challenge for the Agency. Moving forward, we will continue to examine NASA's information security program both through focused audits of discrete issues and future FISMA reviews.

**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).*

We appreciate the courtesies extended to our team during this review. If you have questions about this memorandum, please 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: Renee Wynn
Chief Information Officer

Joseph Mahaley
Assistant Administrator for Protective Services

Enclosures – 3

*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 2016 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

The Office of Management and Budget (OMB), Department of Homeland Security (DHS), and Council of the Inspectors General on Integrity and Efficiency developed the FY 2016 FISMA reporting requirements in consultation with the Federal Chief Information Officers Council. This collaboration resulted in two major changes from the previous year's reporting requirements. First, reporting requirements are now aligned to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).[1] The Cybersecurity Framework provides agencies and Inspectors General with a common structure for managing and evaluating information security risks across the enterprise. Second, a scoring system was created to measure the effectiveness of an agency's information security programs on the basis of the maturity level of various aspects of the program.

Cybersecurity Framework

The Cybersecurity Framework includes activities, desired outcomes, and applicable references common across critical infrastructure sectors and focuses on five specific functions critical to an effective information security program: Identify, Protect, Detect, Respond, and Recover.

1. *Identify.* Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. *Protect*. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. *Detect*. Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. *Respond*. Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. *Recover.* Develop and implement the 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 lifecycle of an organization's cybersecurity risk management program.

[1] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014.

The FY 2016 OIG FISMA reporting requirements are organized around these five functions, with each tied to one or more FISMA review areas. For example, the Identify function encompasses both risk management and management of contractor systems. Table 1 depicts the alignment of the Cybersecurity Framework to the FY 2016 OIG FISMA review areas.

Table 1: Alignment of Cybersecurity Framework with OIG FISMA Review Areas

Cybersecurity Framework Functions	FY 2016 OIG FISMA Review Areas
Identify	Risk management
	Contractor systems
Protect	Configuration management
	Identity and access management
	Security and privacy training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

Source: NASA OIG presentation of the FY 2016 FISMA reporting requirements for Inspectors General.

Point Scoring System

OMB and DHS developed a scoring system with point allotments for each of the five functions. Agencies are allotted up to 20 points for each function for a total of 100 points, which represents a fully effective information security system. Agencies gain points by satisfying metrics associated with attainment of the various functions. Accordingly, the more mature an agency's efforts on a particular function, the higher its score for that function.

The point scoring system assesses effectiveness based on five maturity levels: Ad-hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

1. *Ad-hoc (Level 1)*. An agency lacks a formalized program and performs activities in a reactive manner.

2. *Defined (Level 2)*. An agency has a formalized program with comprehensive policies, procedures, and strategies consistent with NIST but fails to consistently implement them organization-wide.

3. *Consistently Implemented (Level 3)*. An agency consistently implements its program but lacks qualitative and quantitative measures and data on its effectiveness.

4. *Managed and Measurable (Level 4)*. An agency uses metrics to measure and manage implementation of its program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

5. *Optimized (Level 5)*. An agency's program is institutionalized, repeatable, self-regenerating, and updated on a near real-time basis based on changes in business or mission requirements and a changing threat and technology landscape.

To be considered effective, an agency must achieve at least Level 4 (Managed and Measurable) on a particular function. Table 2 outlines the scoring methodology associated with the various maturity levels.

Table 2: Point Allotment for Maturity Level Achieved

Maturity Level	Scoring Description	Point Allotment	Cumulative Points
Ad-hoc (Level 1)	Agencies automatically receive 3 points regardless of their performance on the individual Level 1 metrics.	3 points	3 points
Defined (Level 2)	For the Identify, Protect, and Recover functions, agencies must meet at least half of the Level 2 metrics. For the Detect and Respond functions, agencies must meet all Level 1 metrics and at least half the Level 2 metrics.	4 points	7 points
Consistently Implemented (Level 3)	For all functions, agencies must meet all Level 2 metrics and at least half the Level 3 metrics.	6 points	13 points
Managed and Measurable (Level 4)	For all functions, agencies must meet all Level 3 metrics and at least half the Level 4 metrics.	5 points	18 points
Optimized (Level 5)	Agencies must meet Level 4 and 5 metrics for all function areas.	2 points	20 points

Source: NASA OIG presentation of the FY 2016 FISMA reporting requirements for Inspectors General.

OMB and DHS established a set of "maturity model metrics" for Inspectors General to use in applying the Cybersecurity Framework functions. For example, to determine the maturity level of an agency's Identify function, Inspectors General should consider whether that agency (1) has established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and (2) incorporates mission and business process-related risks into risk-based decisions as described in NIST guidelines. Responses to these metrics determine the score an agency receives and therefore its overall maturity level. See Enclosure III for a summary and link to the complete list of these metrics.

RESULTS

For our review, we assessed NASA's information security policies, procedures, and practices and examined five individual information systems. We identified these systems based on an inventory of 462 NASA and contractor information systems the Agency's Office of the Chief Information Officer (OCIO) provided to us. We also reviewed the NASA's progress in addressing issues identified in prior FISMA and other information security reviews.

In sum, we found that NASA lacks an effective program in any of the five functions, earning 27 of the possible 100 maturity level points. As shown in Table 3, for the Protect and Detect functions, the Agency's program is at Level 1 and for the Identify, Respond, and Recover functions at Level 2. That said, we noted NASA has several efforts underway to improve its information security program.

Table 3: Level of Maturity Point Allotment for NASA

Function	Maturity Level	Points Awarded	Possible Points
Identify	Level 2: Defined	7	20
Protect	Level 1: Ad-hoc	3	20
Detect	Level 1: Ad-hoc	3	20
Respond	Level 2: Defined	7	20
Recover	Level 2: Defined	7	20
Total		**27**	**100**

Source: OIG.

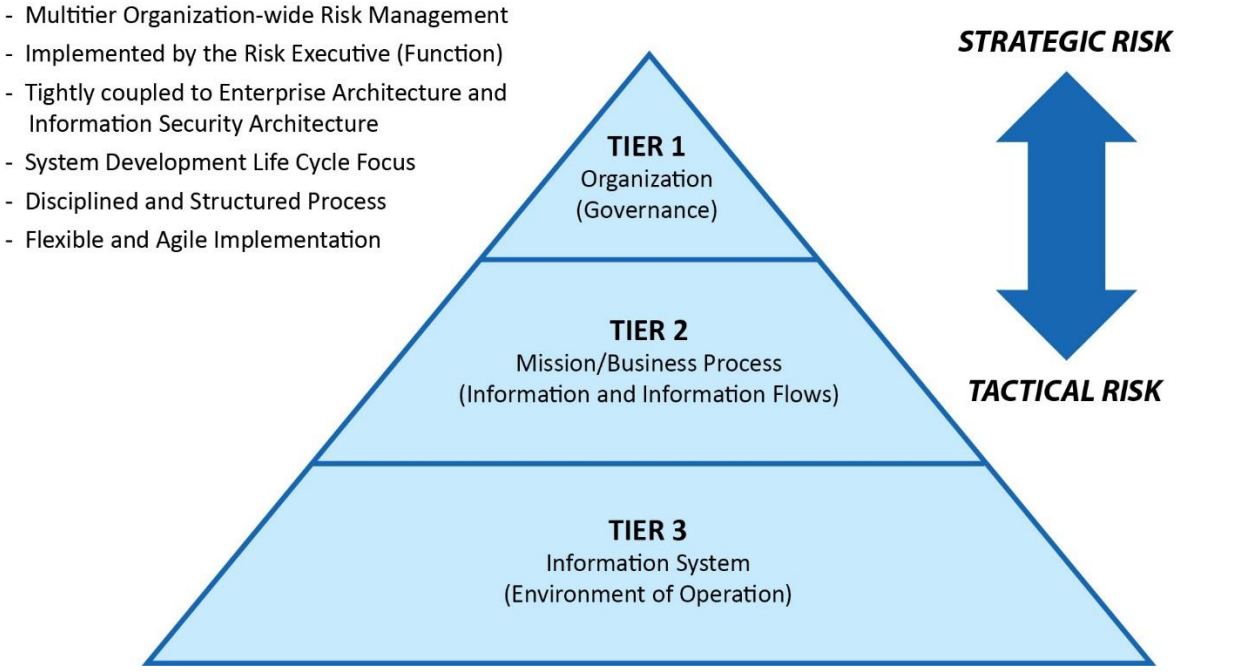
1. Identify

The activities associated with the Identify function – risk management and management of contractor systems – are foundational for effective use of the Cybersecurity Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Based on our review of NASA's efforts in these two review areas, the Agency scored 7 out of 20 points for the Identify function, which placed the Agency at Level 2 (Defined) for that function.

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. The risk management process must be integrated throughout the organization, employing a tiered approach that addresses risk at the organization, mission/business process, and information system levels (see Figure 1). The maturity model for risk management includes metrics related to an organizational level risk management strategy, system interconnections, and an insider threat detection and prevention program. For the reasons discussed below, we found NASA lacks an Agency-wide risk management framework for information security, has not properly managed information system connections between the Agency's Near Earth Network and the external entities supporting that Network's operations, and has yet to fully implement an insider threat detection and prevention program.

Figure 1: Three-Tiered Approach to Risk Management



Source: NASA presentation of NIST SP 800-37 information.

In our FY 2011 through FY 2015, FISMA reviews, we reported OCIO officials had not developed an Agency-wide risk assessment process specific to information security. In addition, we identified specific areas where NASA could improve its risk management program in six other reviews performed over the past 5 years.

1. In a June 2013 audit, we found NASA's information technology (IT) governance structure ineffective due to the decentralized nature of Agency operations and its longstanding culture of autonomy.[2] As a result, NASA did not have a complete inventory of IT assets and the Agency Chief Information Officer (CIO) was unable to enforce security measures over a majority of those assets. Moreover, the lack of visibility into NASA's inventory of IT assets made it difficult for the Agency to conduct a thorough risk assessment of its IT security. We recommended the NASA Administrator consolidate IT governance in the OCIO to ensure appropriate visibility, accountability, and integration of all Mission-related IT assets and activities. In FY 2016, the Agency implemented an adapted version of an IT governance model approved by the Mission Support Council and we closed our recommendation. We are performing a follow-up audit that should be released in the first half of 2017 to examine the efforts NASA has made to improve its IT governance since issuance of our 2013 report.[3]

[2] NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

[3] NASA OIG Assignment No. A-16-013-00, "Audit of NASA's Efforts to Improve the Agency's Information Technology Governance," announced March 31, 2016.

2. In a February 2014 audit, we evaluated NASA's management of smartphones, tablets, basic cell phones, and AirCards.[4] These mobile devices pose security threats because of their size, portability, constant wireless connection, physical sensors, and location services. Further, the diversity of available devices, operating systems, carrier-provided services, and applications present additional security challenges. We found that although NASA began enforcing security requirements on all smartphones and tablets that connect to NASA's e-mail systems in September 2013, the Agency still needed to implement a tool to mitigate risks when those devices connect to NASA systems other than e-mail. In response to our recommendations, the Agency has been reviewing various tools and plans to complete corrective action in October 2017, which should result in a single, comprehensive inventory of mobile devices – both NASA-furnished and personal – that access Agency IT systems.

3. In a July 2014 audit, we highlighted deficiencies with risk assessment controls on certain wide area network infrastructure associated with the Space Network and the White Sands Complex *Redaction pursuant to exemption (b)(7)(E) of the FOIA.* .[5] NASA officials partially concurred with our recommendation and stated they planned to review policies for possible updating and complete required revisions by January 2018.

4. In another July 2014 audit, 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.[6] These deficiencies occurred because NASA did not prioritize identification of security vulnerabilities by seriousness of potential impact, identify the underlying cause of vulnerabilities, identify weaknesses associated with unsound IT security practices, or implement an effective process to ensure timely mitigation of identified vulnerabilities. We made five recommendations to improve risk management in the Agency's 1,200 publicly accessible web applications. During FY 2015, NASA completed corrective actions to address three of our recommendations. However, NASA must still remove from the Internet or secure with a web application firewall all Agency web applications in development or testing mode as well as ensure that critical and high-severity web application vulnerabilities are mitigated within Agency timeframes. NASA plans to complete corrective actions by July 2017.

5. In a March 2016 audit, we found NASA's decision to assign a security categorization rating of "Moderate" rather than "High" to the Near Earth Network's IT systems was based on flawed justifications and resulted in the Network being excluded from the Agency's Protection Program.[7] We also determined information system connections between the Network and the external entities that support its operations were not managed in accordance with Federal and NASA policy. We made 10 recommendations to ensure NASA is properly protecting the

[4] NASA OIG, "NASA's Management of its Smartphones, Tablets, and Other Mobile Devices" (IG-14-015, February 27, 2014). An AirCard is a device that provides the user with access to wireless broadband cellular services.

[5] NASA OIG, "Audit of the Space Network's Physical and Information Technology Security Risks" (IG-14-026, July 22, 2014).

[6] NASA OIG, "Security of NASA's Publicly Accessible Web Applications" (IG-14-023, July 10, 2014).

[7] NASA OIG, "NASA's Management of the Near Earth Network" (IG-16-014, March 17, 2016).

Network. NASA has completed corrective action to address one recommendation and has plans to complete corrective actions related to the other recommendations.[8]

6. In April 2016, we reported that although NASA had made progress in meeting requirements in support of an Agency-wide information security program, the Agency had not fully implemented key management controls essential to managing that program.[9] Specifically, NASA lacked an Agency-wide risk management framework for information security and supporting architecture. We determined this condition existed because the OCIO had not developed an information security program plan to effectively manage its resources. In addition, the Office was experiencing a period of transition with different leaders acting in the Senior Agency Information Security Officer role that caused uncertainty surrounding information security responsibilities at the Agency level. To improve management of NASA's information security program, we recommended the NASA CIO direct the Senior Agency Information Security Officer to develop and disseminate an Agency-wide information security program plan that meets NIST requirements. NASA plans to complete corrective actions by December 2019.

In addition to our work, in a May 2016 audit of selected high impact IT systems, the Government Accountability Office (GAO) noted 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.[10] GAO also found NASA assessments were not comprehensive and did not identify many access control weaknesses in its systems. If security assessment plans do not identify controls to be assessed or the procedures to be used, NASA officials cannot be assured that controls are operating as intended. Further, without comprehensive assessments NASA may not be aware of additional control weaknesses that could endanger the confidentiality, integrity, and availability of sensitive data. GAO recommended NASA update security assessment plans for selected systems to ensure they include test procedures and re-evaluate security control assessments for selected systems to ensure they comprehensively test technical controls.

An important part of any agency's risk management process is the plan of action and milestones (POA&M) process to track and prioritize potential security problems. NIST requires agencies to develop a POA&M for the information system 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 in the system. 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. IT system owners and

---

[8] The Associate Administrator for Human Exploration and Operations and the CIO agreed to re-categorize the portion of the Network that supports the Space Launch System and Orion as a "High" system, but intend to retain the "Moderate" rating for the rest of the Network on the grounds it is not critical to the operation of any NASA spacecraft or spacecraft program. The OIG does not believe the Network operates simply as a "pass through" for communications. Rather, Network components must store (albeit temporarily) and process data and commands prior to transmitting to the spacecraft. Given the importance of the Network to the success of NASA Earth science missions and the launch and contingency support it provides other Federal agencies, the OIG continues to believe the entire Network should be categorized as "High."

[9] NASA OIG, "Review of NASA's Information Security Program" (IG-16-016, April 14, 2016).

[10] GAO, "Agencies Need to Improve Controls over Selected High-Impact Systems" (GAO-16-501, May 18, 2016).

other officials use POA&Ms to manage and track completion of corrective actions. All five systems we examined for this review had current POA&Ms.[11]

In sum, while NASA has established a risk management program consistent with FISMA requirements, the program lacks an integrated Agency-wide risk management strategy to support information security continuous monitoring.

Contractor Systems

Federal agencies are responsible for managing the risk of contractor information systems. Among the FISMA metrics for contractor systems are whether "contractor-operated systems are being managed to ensure that they have adequate security" and whether "the organization can make an informed decision about whether to accept any residual risk."

We examined two contractor information systems at the Jet Propulsion Laboratory (JPL) to determine whether NASA (1) established a program to oversee contractor systems; (2) implemented a process to ensure contracts include appropriate information security and privacy requirements; (3) specified within appropriate agreements how information security performance is measured, reported, and monitored; and (4) obtained sufficient assurance that the security controls of contractor systems meet FISMA requirements, OMB policy, and applicable NIST guidelines. We found both systems consistent with applicable requirements.

Nevertheless, we found NASA has failed to follow established Agency policies, standards, and governance methodologies for the security of the Deep Space Network's IT and physical infrastructure. In a March 2015 audit of JPL's Deep Space Network, we identified issues with IT system security categorization, database inventory, vulnerability identification and mitigation practices, and security configuration baselines.[12] In addition, NASA's Security Operations Center (SOC) was not adequately integrated into JPL's computer network operations. We made six recommendations to ensure Deep Space Network personnel follow established IT security policies, standards, and governance methodologies and develop a strategy for implementing evolving IT security policies at JPL. NASA and JPL plan to complete corrective actions by September 2017.

2. Protect

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the areas of configuration management, identity and access management, and security and privacy training. Based on our review of NASA's efforts in those areas, the Agency scored 3 of 20 possible points for the Protect function, which placed the Agency at Level 1 (Ad-hoc) for that function.

[11] As part of our ongoing follow-up audit of NASA's IT governance, we are reviewing the POA&M for two additions systems, both of which are associated with the Agency Consolidated End-User Services contract. In July 2016, the NASA CIO authorized the two systems to operate with a set of conditions that the support contractor, Hewlett Packard Enterprise Services, must remediate before January 25, 2017.

[12] NASA OIG, "NASA's Management of the Deep Space Network" (IG-15-013, March 26, 2015).

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 given product patches, fixes, and updates. As changes to information systems are made, baseline configurations are updated; specific configuration settings confirmed; and configuration items 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.

When establishing baseline configurations, NASA consults a variety of sources, including NIST guidance, Center for Internet Security (CIS) benchmarks, and industry best practices. Starting in 2005, NASA established "security baselines" that automatically report the configuration settings on Agency information systems. Where a NASA security baseline does not exist, the Agency 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.

In a March 2016 audit, 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 cyber attack.[13] We recommended NASA implement security baselines to the fullest extent possible on Network systems, assess the baselines for changes on a scheduled basis, and develop a process for reporting compliance with security baselines on Network components. NASA plans to complete corrective actions in FY 2018.

More broadly, NASA continues to struggle with implementing secure configuration settings in an environment with diverse operating systems and applications. For example, during this year's review the compliance rate with NASA security baselines averaged 78 percent for Windows devices. However, for Windows servers – considered a higher risk because they provide services to other computer devices over a network and include web servers – the compliance rate for implementation of secure configuration settings was only 46 percent.

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.

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 Number 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.[14] HSPD-12 requires agencies, to the maximum extent practicable, to follow specific technical standards and business processes when issuing

[13] IG-16-014.

[14] HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

Federal Personal Identity Verification (PIV) credentials, including standard background investigations to verify the identities of employees and contractors.[15]

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 to Federal information systems.[16] 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/sensitivity, and information about the individual's background investigation. This information is used to determine what systems (physical and logical) an individual may access.
2. *Credential management* identifies what media (hard or soft) may be used to permit physical or logical 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.

We found appropriate identity and access controls were in place for each of the five information systems reviewed. NASA uses the electronic capabilities of the PIV credentials combined with visual authentication for physical access to Agency facilities. Additionally, NASA has deployed software and hardware to enable PIV-based access to its systems and networks.

In June 2015, as part of the 30-day Cybersecurity Sprint, OMB required Federal agencies to tighten access for privileged users and increase the use of multi-factor authentication.[17] NASA acquired a tool

---

[15] Exceptions to using PIV credentials are permitted for extenuating circumstances (e.g., a system is in the process of being decommissioned). 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.

[16] 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.

[17] In June 2015, OMB ordered a 30-day Cybersecurity Sprint as a result of a massive breach in Office of Personnel Management information systems. The exercise required all Federal agencies to take immediate and specific actions to improve the security of their information systems and data. A privileged user is someone authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

that enhances its use of PIV credentials and allows privileged users to access Agency systems via PIV-based authentication. As a result, NASA achieved 100 percent PIV authentication for its privileged users. Moreover, NASA increased the use of PIV authentication for its non-privileged users from 76 percent to 82 percent. *Redaction pursuant to exemption (b)(7)(E) of the FOIA.*

NASA has implemented a variety of controls, including firewalls, routers, and authentication servers to enable secure remote access to the Agency's information system through external networks including the Internet. NASA also plans to improve the security posture of the Agency's external and internal networks. For example, NASA plans to deploy a network access control solution that authenticates, assesses, validates, and places network-connecting endpoints and users into network zones commensurate with applicable security policy. Additionally, to ensure consistent implementation, the Agency plans to deploy enterprise firewall and virtual private network services.

In sum, the NASA identity and access management program includes an implementation plan to improve its use of NASA and non-NASA credentials for physical and logical access to information systems. We believe the Agency has made some 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 credentials on Apple machines.

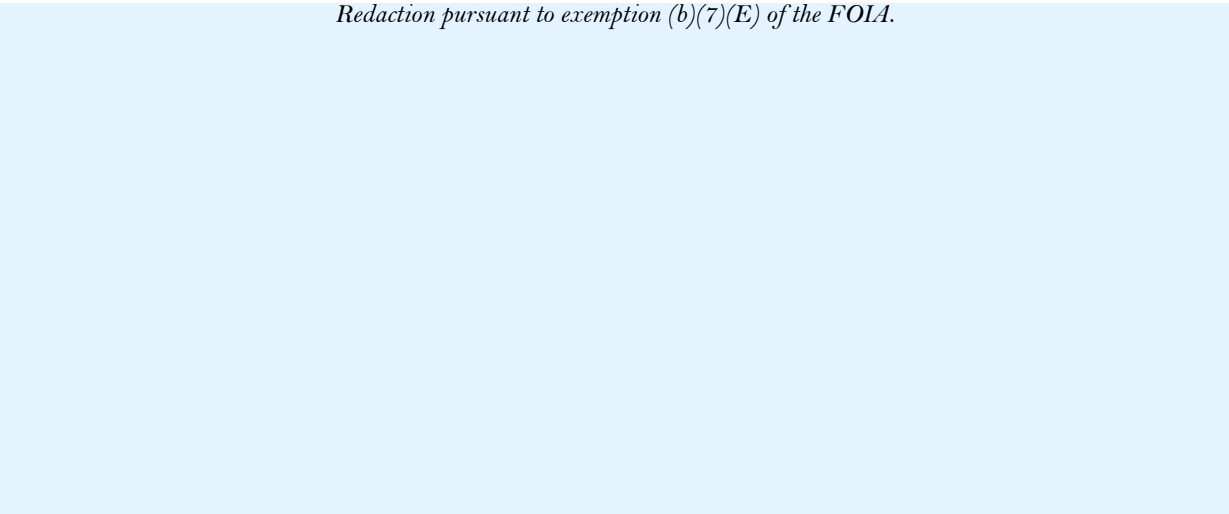
Security and Privacy Training

Some of the most effective attacks on computer networks exploit user behavior through phishing, social engineering to obtain passwords, and introduction of malware via removable media. To help prevent such attacks, and consistent with Federal guidance, NASA requires all users to complete annual online security awareness training available on the Agency's System for Administration, Training, and Educational Resources (SATERN) website. Users with significant information security responsibilities or elevated access to NASA information must complete additional security training appropriate for their roles, including operating system security and IT security for administrators.

The NASA OCIO regularly conducts social engineering exercises, including phishing, malicious media distribution, and tailgating to test its ability to gain unauthorized physical access to 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 NASA SOC conducts quarterly phishing exercises that target large segments of the NASA general IT user population as a means of assessing user-awareness and the effectiveness of the social engineering training and phishing e-mail awareness integrated into the NASA IT Security Awareness training. *Redaction pursuant to exemption (b)(7)(E) of the FOIA.*

Figure 2: FY 2016 Third Quarter Results of NASA Phishing Exercises



Source: NASA OIG presentation of the data provided by NASA.

We interviewed NASA personnel, examined documentary evidence, and performed a limited test of compliance with training requirements. Specifically, we reviewed NASA information security training handbooks, training requirements posted in SATERN, and reports showing personnel who have completed security training. We found that 98 percent of NASA and contractor personnel had completed the required training as of August 15, 2016. However, in our review of contractor systems, we found JPL is not required to identify and track the status of specialized security and privacy training for all personnel with significant information security and privacy responsibilities that require specialized training.

In a May 2016 audit, GAO indicated that although NASA developed and documented comprehensive Agency-wide information security programs, it had not effectively implemented elements of the programs' role-based training to ensure individuals with significant security responsibilities carry out their duties.[18] Specifically, GAO found 25 NASA individuals who had not completed training because until May 2015, Agency officials had not clearly defined role-based training requirements and were still in the process of implementing the requirements specified in the training handbook.

In sum, although NASA is maintaining an information security training program consistent with FISMA requirements, the Agency continues to face significant challenges regarding secure configuration settings, hardware and software asset management, and configuration-related vulnerabilities. NASA also needs to enhance its non-privileged PIV credentials implementation and role-based training.

3. Detect

The Detect function enables timely discovery of cybersecurity events and encompasses continuous monitoring activities. Based on our review of NASA's continuous monitoring efforts, the Agency scored 3 of 20 possible points for the Detect function, which placed the Agency at Level 1 (Ad-hoc) for that function.

[18] GAO-16-501.

Information Security 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 continue to be effective over time in light of changes to system hardware or software. A well-designed and well-managed continuous monitoring program can transform an otherwise static security control assessment and risk determination process into a dynamic 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 their information systems' security controls and ensure system changes do not have a significant impact on security, security plans remain effective, and security controls continue to perform as intended.[19] 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 risk, but not less than annually.

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

- instill a clear understanding of organizational risk tolerance and help officials set priorities and manage risk consistently throughout the organization;
- include metrics that provide meaningful indications of security status at all organizational tiers;
- ensure continued effectiveness of all security controls;
- ensure compliance with information security requirements derived from organizational missions or business functions, Federal legislation, directives, regulations, policies, and standards/guidelines;
- include all organizational information assets and help maintain visibility into the security of the assets;
- ensure knowledge and control of changes to organizational systems and environments of operation; and
- maintain awareness of threats and vulnerabilities.

In our FY 2014 FISMA review, we found that although NASA had documented a high-level ISCM strategy, it would benefit from creating a more detailed strategy by including implementation details for the role of the "Risk Executive" and how existing capabilities support the Agency's ISCM program.

---

[19] OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996.

[20] 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.

[21] NIST named the individual who oversees an organization's ISCM strategy and program as the "Risk Executive."

In this review, we found NASA has not defined and communicated across the Agency the identities and responsibilities of ISCM stakeholders or how it will integrate ISCM activities with Agency risk tolerance, the threat environment, and business or mission requirements. In addition, we found NASA has not yet identified and defined the qualitative and quantitative performance measures it will use to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. NASA has also not defined its processes for collecting and considering lessons learned to improve ISCM processes.

DHS, in partnership with the General Services Administration, established a Government-wide acquisition vehicle for a continuous diagnostics and mitigation (CDM) program. The first phase of the CDM program is expected to provide Federal agencies with capabilities and commercial off-the-shelf tools that enable system and network administrators to know what is connected to their networks, current vulnerabilities, and configuration management. This should allow each agency to identify and rank problems for priority resolution. In September 2015, DHS awarded a task order to Booz Allen Hamilton (Booz Allen) to implement CDM services at NASA and several other agencies. NASA OCIO officials told us they worked with Booz Allen and Center personnel in FY 2016 to identify the ISCM technologies needed for asset management and to integrate the necessary IT security tools and services. NASA plans to complete CDM implementation in FY 2017.

In sum, while NASA has established an enterprise-wide continuous monitoring program consistent with FISMA requirements, the Agency needs to improve its ISCM program by developing comprehensive, Agency-wide ISCM policies, procedures, and strategies.

4. Respond

The Respond function supports the ability to contain the impact of a potential information security incident and focuses on incident response. Based on our review of NASA's incident response efforts, the Agency scored 7 of 20 possible points for the Respond function, which placed the Agency at Level 2 (Defined) for that function.

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 cyber attacks. 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, which is used to coordinate, track, and report information security incidents.

NASA SOC

Source: NASA.

In an August 2012 audit, we found several areas in which NASA could improve its incident response and reporting program.[22] Specifically, even though each of the six mission networks we reviewed had their own incident management program that included network monitoring, dedicated staff to respond to incidents, and documented processes, these programs did not provide the type of centralized continuous monitoring coverage offered by the SOC. In addition, we noted NASA needed to increase its readiness to combat the sophisticated and increasingly common form of cyber attack known as Advanced Persistent Threats.[23] *Redaction pursuant to exemption (b)(7)(E) of the FOIA.*

In this review, we found NASA is detecting, tracking, and responding to incidents but has not fully implemented malware and other network defense technologies that could improve the overall effectiveness of these actions. To remediate this condition, Agency officials said several tools would be implemented in FY 2017 to improve detection of suspicious activities and data loss prevention.

In sum, while NASA is maintaining an incident response and reporting program consistent with FISMA requirements, the program needs improvement to ensure sufficient incident monitoring and detection coverage *FOIA (b)(7)(E).* . We will continue to work with the OCIO to verify appropriate corrective actions are taken and new technologies to detect and investigate suspicious activities are fully implemented.

5. Recover

The Recover function supports timely recovery to normal operations in order to reduce the impact from a cybersecurity event by focusing on contingency planning. Based on our review of NASA's contingency planning efforts, the Agency scored 7 of 20 possible points for the Recover function, which placed the Agency at Level 2 (Defined) for that function.

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 alternative site, recovery of information system functions using alternative equipment, or performance of information system functions using manual methods.

[22] NASA OIG, "Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 7, 2012).

[23] Advanced Persistent Threats are cyber attacks tailored to the target organization's systems. Such attacks are designed to bypass the target's firewalls, intrusion detection systems, and other perimeter defenses and typically are launched by well-organized and well-funded individuals or entities.

We examined contingency planning controls such as maintenance and testing of current contingency plans for the five selected information systems and found that all had appropriate controls.

However, while NASA is maintaining an Agency-wide business continuity and disaster recovery program consistent with FISMA requirements, *Redaction pursuant to exemption (b)(7)(E) of the FOIA.* .

CONCLUSION

NASA received 27 out of 100 possible maturity level points, indicating that overall it has not yet implemented an effective information security program. To improve its information security program, we believe the Agency should

- implement an integrated Agency-wide risk management strategy and obtain sufficient assurance that the security controls of systems operated by contractors meet FISMA requirements;
- fully implement secure configuration settings, improve hardware and software asset management; remediate configuration-related vulnerabilities; and enhance non-privileged PIV credentials implementation and role-based training;
- develop comprehensive, Agency-wide ISCM policies, procedures, and strategies;
- ensure sufficient incident monitoring and detection coverage *FOIA (b)(7)(E).* ; and
- *Redaction pursuant to exemption (b)(7)(E) of the FOIA.* .

Enclosure II: Scope and Methodology

We performed this review from February through November 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 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.

We evaluated the effectiveness of NASA's information security program and practices. We followed the instructions dated September 26, 2016, from DHS's Office of Cybersecurity and Communications. We used a comprehensive review approach designed to identify deficiencies concurrently for all five FISMA functional areas. Specifically, we reviewed a sample of five Agency and contractor information systems for compliance with FISMA along with NASA, NIST, and OMB requirements. We reviewed relevant documentation, including information system security plans, risk assessment reports, security assessment reports, accreditation decision letters, POA&Ms, and SOC reports. We did not evaluate the technical adequacy of those documents other than to determine whether they generally met NIST and OMB guidelines. In addition, we interviewed NASA security officials and staff at Headquarters, the NASA Centers, and JPL. We also determined whether deficiencies identified in the FY 2015 FISMA review continued to exist. Further, we assessed the impact of recently completed or ongoing NASA OIG audits. Lastly, we performed work to address FY 2016 DHS requirements within the five Cybersecurity Framework functions.

Federal Laws, Regulations, Policies, and Guidance

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 (HSPD) 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
- HSPD-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, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010
- NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011
- NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," June 2009
- NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
- NIST SP 800-53A, Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," December 2014
- NASA Policy Directive (NPD) 1600.2E, "NASA Security Policy (Revalidated on 4/2/2015 w/Change 1)," April 28, 2004
- 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) 1382.1A, "NASA Privacy Procedural Requirements," July 10, 2013
- NPR 1600.2, "NASA Classified National Security Information," October 11, 2011
- 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
- NPR 2841.1, "Identify, Credential, and Access Management," January 6, 2011
- NASA OCIO IT Security Division Standard Operating Procedure ITS-SOP-2810.02-01 V2, "Security Assessment and Authorization: Internal Information Assurance Review," June 30, 2016
- NASA Handbook ITS-HBK-2810.02-02, "Information System Security Assessment and Authorization Process," February 1, 2015
- ITS-HBK-2810.02-04A, "Continuous Monitoring – Security Control Ongoing Assessments and Authorization," March 18, 2014
- ITS-HBK-2810.02-05A, "Security Assessment and Authorization: External Information Systems," October 11, 2016
- ITS-HBK-2810.02-08A, "Security Assessment and Authorization: Plan of Action and Milestone (POA&M)," July 31, 2015

- ITS-HBK-2810.06-01, "Security Awareness and Training," May 6, 2011
- ITS-HBK-2810.06-02, "Awareness and Training: Role Based Training," February 5, 2016
- ITS-HBK-2810.07-01, "Configuration Management," May 6, 2011
- ITS-HBK- 2810.08-01, "Contingency Planning," May 6, 2011
- ITS-HBK-2810.09-01A, "Incident Response and Management," December 30, 2014
- ITS-HBK-2810.15-01A, "Access Control," September 4, 2012
- ITS-HBK-2810.17-01, "Identification and Authentication," January 17, 2011
- ITS-HBK-2841-002, "Identity, Credential, and Access Management (ICAM) Services," March 9, 2016

Review of Internal Controls

We evaluated internal controls related to the five FISMA function areas. In addition, we evaluated internal controls related to the assessment and authorization of five information systems. As discussed in Enclosure I, we found that internal controls in some areas needed improvement.

Prior Coverage

During the last 5 years, the NASA OIG and the 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/FY17 and http://www.gao.gov, respectively.

NASA Office of Inspector General

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)

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)

Government Accountability Office

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

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)

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 III: FY 2016 IG Reporting Requirements by Level, Number of Metrics, and Possible Points

Level	Number of Metrics	Possible Points
Identify		
Level 1: Ad-hoc	0	3
Level 2: Defined	4	4
Level 3: Consistently Implemented	11	6
Level 4: Managed and Measureable	6	5
Level 5: Optimized	Achieve 100% of Level 4 capabilities	2
Level 5: Optimized		**20**
Protect		
Level 1: Ad-hoc	0	3
Level 2: Defined	5	4
Level 3: Consistently Implemented	18	6
Level 4: Managed and Measureable	8	5
Level 5: Optimized	Achieve 100% of Level 4 capabilities	2
Level 5: Optimized		**20**
Detect		
Level 1: Ad-hoc	10	3
Level 2: Defined	10	4
Level 3: Consistently Implemented	10	6
Level 4: Managed and Measureable	12	5
Level 5: Optimized	7	2
Level 5: Optimized		**20**
Respond		
Level 1: Ad-hoc	12	3
Level 2: Defined	12	4
Level 3: Consistently Implemented	13	6
Level 4: Managed and Measureable	9	5
Level 5: Optimized	8	2
Level 5: Optimized		**20**
Recover		
Level 1: Ad-hoc	0	3
Level 2: Defined	2	4
Level 3: Consistently Implemented	6	6
Level 4: Managed and Measureable	3	5
Level 5: Optimized	Achieve 100% of Level 4 capabilities	2
Level 5: Optimized		**20**

Source: NASA OIG analysis.

Note: For a complete list of the FY 2016 IG FISMA metrics, go to https://www.dhs.gov/sites/default/files/publications/FY%202016%20IG%20FISMA%20Metrics%20508%20compliant%20.pdf (last accessed, November 2, 2016).