NASA OFFICE OF INSPECTOR GENERAL

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

July 27, 2016

The Honorable Richard Shelby
Chairman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Barbara Mikulski
Vice Chairwoman
Subcommittee on Commerce, Justice,
Science and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

Subject: *Report Mandated by the Cybersecurity Act of 2015* (IG-16-026)

Dear Mr. Chairman and Madame Vice Chairwoman,

This letter responds to the requirement in the Cybersecurity Act of 2015 (Act) that directs the NASA Office of Inspector General (OIG) to report on the Agency's information technology (IT) security practices for protecting data in "covered systems," defined as a national security system or a Federal system that provides access to personally identifiable information.[1]

[1] Public Law No. 114-113, Division N, December 18, 2015. A national security system is defined in 40 U.S. Code § 11103 as a telecommunications or information system operated by the Federal Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions.

Background

Since 2006, the OIG has identified "securing NASA's IT systems and data" as a top management challenge.[2] In addition, over the last 6 years the OIG issued 21 audit reports containing 85 recommendations designed to improve NASA's IT security efforts.[3] For example, we highlighted issues related to acquisition of IT systems, cybersecurity vulnerabilities, IT security incident detection and handling capabilities, continuous monitoring tools, cloud computing technologies, web application security, and overall NASA IT governance.

Section 406 of the Cybersecurity Act of 2015 requires Inspectors General to submit reports to Congress describing Agency IT security policies, procedures, and practices in the following areas:

- **Logical access controls**. The processes of granting or denying requests to obtain and use electronic information and systems.
- **Multi-factor authentication**. The use of at least two authentication factors, such as passwords and identification badges, to obtain access to IT resources.
- **Software inventory**. The conduct of software inventory and their associated licenses.
- **Threat monitoring and detection**. The capability to not only detect threats, but prevent data loss, employ forensics, and manage digital rights.
- **Contractor oversight**. The process and procedures to ensure contractors are implementing information security management practices.

Logical Access Controls

The Act requires a description of Agency policies and practices for logical access controls on covered systems, a description of logical access controls for privileged users, and a determination of whether appropriate standards were followed.

NASA policies and practices for logical access controls on its covered systems include:

- NASA Procedural Requirements (NPR) 1382.1A, "NASA Privacy Procedural Requirements," establishes policies and practices for protecting personally identifiable information.
- NPR 1600.2, "NASA Classified National Security Information (CNSI) w/Change 2 (2/12/2014)," establishes policies and practices for protecting CNSI.
- NPR 2810.1A, "Security of Information Technology," establishes policies and practices for logical access controls for users, including privileged users. This NPR requires account management capabilities (e.g., account creation, maintenance, and deletion) to be in place for Agency information systems.

[2] The Reports Consolidation Act of 2000 requires the OIG to provide its views on the top management and performance challenges facing NASA. Our reports on this subject can be found at https://oig.nasa.gov/challenges.html.

[3] OIG audit reports can be found at https://oig.nasa.gov/audits/reports/FY16/index.html.

- NPR 2841.1, "Identity, Credential, and Access Management," establishes policies and practices to manage identity, credential, and access management services as an integrated end-to-end service to improve security, efficiency, and collaboration within the Agency.
- NASA Handbook ITS-HBK-2810.15-01A, "Access Control," establishes policies and practices for logical access controls for users, including privileged users. This handbook derives requirements and recommendations for logical access controls from the National Institute of Standards and Technology.[4]
- NASA Handbook ITS-HBK-2810.17-01, "Identification and Authentication," establishes policies and practices for logical access controls for users, including privileged users, and provides guidance to confirm the identity of a user requesting access to NASA resources (e.g., a person logging in to a computer or a laptop computer connecting to a wireless network). These controls address the creation, management, usage, and protection of identities (e.g., usernames) and authenticators (e.g., smart cards and tokens).
- NASA Handbook ITS-HBK-2841-002, "Identity, Credential, and Access Management (ICAM) Services," provides guidance for implementing logical access management as an Agency service.

Logical access controls for privileged users include: (1) enforcing user authentication for access, (2) restricting the number of unsuccessful login attempts, (3) displaying a notice for system use and a warning banner, (4) locking a user session after a specified time limit for inactivity, and (5) using multi-factor authentication for remote access.

We reviewed a total of four covered systems – one national security system and three systems containing personally identifiable information – and validated the controls in place and also determined appropriate standards were followed.

Multi-factor Authentication

The Act requires a description of multi-factor authentication for access to covered systems by privileged users.

NASA manages access to covered systems by requiring privileged users to use either a token with a personal identification number or a "smartcard" with a personal identification number for multi-factor authentication. During our review of the four covered systems, we verified that NASA used a smartcard with a personal identification number as multi-factor authentication for privileged users.

Software Inventory

The Act requires a description of policies and procedures to conduct inventories of software and associated software licenses.

[4] National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

NASA policies and procedures to conduct inventories of software and the associated software licenses include the following:

- NPR 2810.1A, "Security of Information Technology," provides policies and procedures for inventory and configuration management, and requires maintenance of an information system inventory, including information system components and software inventory.
- NASA Handbook ITS-HBK-2810.07-01, "Configuration Management," identifies policies and procedures for software inventory and requires the Agency to have the capability to automatically collect software data. In addition, the Handbook requires implementation of a licensing management solution that allows for tracking software use and associated documentation protected by quantity licenses in order to control copying and distribution. The Handbook also requires NASA to control and document the use of peer-to-peer file sharing technology to ensure the technology is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.
- NASA operating procedure ITS-SOP-2810.02-01, "OCIO ITSD Standard Operating Procedure (SOP): Internal Information Assurance Review," requires a review of information systems to ensure software inventory is appropriately documented.

Threat Monitoring and Detection

The Act requires a description of capabilities used by the Agency to monitor and detect exfiltration and other cybersecurity threats.[5] These capabilities may include data loss prevention, forensics and visibility, and digital rights management.

The NASA Security Operations Center (SOC) serves as the primary site for Agency-wide IT incident handling and provides centralized, continuous monitoring of computer network traffic entering and leaving NASA Centers. The SOC maintains an information system (the Incident Management System) for Agency-wide coordination, tracking, and reporting of IT security incidents. Located at Ames Research Center, the SOC is designed to detect security incidents, such as the installation of malware or denial of service attacks, and deploy computer forensics capabilities to provide assistance in investigating cyber-attacks and preserving cyber evidence.

According to NASA officials, the Agency uses a variety of tools to monitor traffic on its networks and alert SOC team members if an anomaly, such as attempted data exfiltration, has been detected. NASA also uses software tools to proactively identify and block malware and other forms of malicious network activity before cyber criminals attempt to exfiltrate data from the network. Agency desktops, laptops, and servers also have antivirus/malware detection software to detect and quarantine known malicious software activities. Moreover, NASA uses internet content filtering tools to block access to known malicious sites, as well as tools to help detect when malicious activities take place and notify IT staff to take action to remediate the incident.

[5] Exfiltration, also called data extrusion, is the unauthorized transfer of data from a computer. Such a transfer may be manual and carried out through physical access to a computer or it may be automated and carried out through malicious programming over a network.

Regarding forensics and visibility, NASA officials stated that the Agency has tools for capturing data packets and traffic analysis to investigate IT security incidents on the network. NASA also uses tools to perform forensic examinations without compromising the integrity of an infected system.

NASA officials stated they are not aware of requirements for digital rights management, and noted that the Agency has encryption solutions to protect personally identifiable information and classified information.

Contractor Oversight

The Act requires a description of policies and procedures to ensure entities providing services to NASA, including contractors, implement IT security management practices, including software inventory and threat monitoring and detection. As part of this review, we interviewed NASA and contractor employees responsible for implementing the security controls on our sampled systems.

NASA policies and procedures for contractor oversight include:

- NPR 1382.1A, "NASA Privacy Procedural Requirements," identifies policies and procedures for oversight of contractor services requiring access to personally identifiable information. Notification must be made to the contracting officer when contractor services will require or include access to personally identifiable information collected by or on behalf of NASA. In addition, the contract's statement of work must identify NPR 1382.1A as a requirement the contractor must follow.
- NASA Policy Directive 1600.2E, "NASA Security Policy (Revalidated on 4/2/2015 w/Change 1)," requires appropriate personnel security and oversight of non-NASA civil servants including contractors, grantees, and foreign nationals requiring access to NASA covered systems.
- NPR 1600.2, "NASA Classified National Security Information (CNSI) w/Change 2 (2/12/2014)," requires periodic reviews to ensure CNSI is properly protected against unauthorized disclosure or access. This NPR also requires that requests for proposal or offer include a statement whether the contractor or prospective contractor will require access to classified information and generate classified information in performance of such contract. If the contract involves access to classified information, a letter requiring that each contractor comply with the National Industrial Security Program Operating Manual will be part of the contract negotiation. This NPR also requires each classified contract to contain the standard security clauses prescribed by the NASA Federal Acquisition Regulation Supplement Subpart 1852.204-75, Security Classification Requirements.
- NASA Policy Directive 2810.1E, "NASA Information Security Policy," requires NASA to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access of information collected or maintained by or on behalf of NASA within information systems used or operated by the Agency, a NASA contractor, or another organization on behalf of NASA.
- NPR 2810.1A, "Security of Information Technology," establishes contractor oversight by ensuring the information security requirements are documented in solicitations and resulting contracts for acquisitions made in support of covered systems. The principal information

security clause to be included with contracts, grants, and other agreements is defined by the Federal Acquisition Regulation clause and applicable Procurement Information Circular Information Technology Security Requirements.

- NASA Handbook ITS-HBK-2810.02-05A, "Security Assessment and Authorization: External Information Systems," defines an external information system as any information system owned, operated, and managed by outside agencies, contractors, universities, or other organizations that store, process, or disseminate NASA-owned data under a contract or formal agreement with the Agency. This Handbook requires the Federal Acquisition Regulation clause for information security be included in contracts for external information systems. The NASA Federal Acquisition Regulation Information Technology Security Clause requires an Information Technology Security Management Plan for each contract and an Information Technology Security Plan for each information system.

To meet the requirements of the Act, we conducted our review work in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the review to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings and conclusions. We believe the evidence obtained provides a reasonable basis for our response to the reporting requirements.

Because the Act primarily requires a description of Agency policies and procedures, we generally did not evaluate their adequacy or effectiveness of implementation as part of this review. However, as discussed earlier in this report, we have examined many of these issues in depth in audit reports issued over the preceding 6 years.

See Enclosure II for a list of NASA policies, procedures, and practices applicable to the Cybersecurity Act of 2015.

If you or your staff have questions about this report or need additional information, please contact me or Renee Juhans, OIG Executive Officer, at 202-358-1220.

Sincerely,

Paul K. Martin
Inspector General

cc: Charles F. Bolden, Jr.
Administrator

Dava Newman
Deputy Administrator

Robert Lightfoot
Associate Administrator

Michael French
Chief of Staff

Renee Wynn
Chief Information Officer

Al Condes
Associate Administrator, International and Interagency Relations

Krista Paquin
Associate Administrator, Mission Support Directorate

Sumara Thompson-King
General Counsel

Enclosure – 2

ENCLOSURE I: CONGRESSIONAL RECIPIENTS

United States Senate

The Honorable John Thune
The Honorable Bill Nelson
The Honorable Ted Cruz
The Honorable Gary Peters
The Honorable Ron Johnson
The Honorable Thomas R. Carper

U.S. House of Representatives

The Honorable John Culberson
The Honorable Michael Honda
The Honorable Jason Chaffetz
The Honorable Elijah Cummings
The Honorable Mark Meadows
The Honorable Gerald Connolly
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson
The Honorable Barry Loudermilk
The Honorable Don Beyer
The Honorable Brian Babin
The Honorable Donna Edwards

ENCLOSURE II: APPLICABLE NASA POLICIES, PROCEDURES, AND PRACTICES

Table 1: NASA Policies, Procedures, and Practices Applicable to the Cybersecurity Act

Policy Number	Policy Title	Effective Date
NPR 1382.1A	NASA Privacy Procedural Requirements	July 10, 2013
NASA Policy Directive 1600.2E	NASA Security Policy (Revalidated on 4/2/2015 w/Change 1)	April 28, 2004
NPR 1600.2	NASA Classified National Security Information	October 11, 2011
NASA Policy Directive 2810.1E	NASA Information Security Policy	July 14, 2015
NPR 2810.1A	Security of Information Technology	May 16, 2006
NPR 2841.1	Identity, Credential, and Access Management	January 6, 2011
ITS-SOP-2810.02-01	OCIO ITSD Standard Operating Procedure (SOP): Internal Information Assurance Review	June 15, 2015
ITS-HBK-2810.02-05A	Security Assessment and Authorization: External Information Systems	February 4, 2016
ITS-HBK-2810.07-01	Configuration Management	May 6, 2011
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

Source: NASA.