National Aeronautics and Space Administration

OFFICE OF INSPECTOR GENERAL

NASA's Management of its Smartphones, Tablets, and Other Mobile Devices

OFFICE OF AUDITS

AUDIT REPORT

FEBRUARY 27, 2014

IG-14-015

(A-12-023-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

ACES	Agency Consolidated End-user Services
CIO	Chief Informatio Officer
CMDB	Configuration Management Database
ESRS	Enterprise Service Request System
HP	HP Enterprise Services
IT	Information Technology
NSSC	NASA Shared Services Center
ODIN	Outsourcing Desktop Initiative for NASA
OIG	Office of Inspector General

OVERVIEW

NASA'S MANAGEMENT OF ITS SMARTPHONES, TABLETS, AND OTHER MOBILE DEVICES

The Issue

Mobile electronic devices, including smartphones and tablets, are key components of NASA's information technology (IT) strategy to provide its employees and contractors flexibility in accessing Agency networks from anywhere at any time. Although mobile devices with computing capabilities offer greater workplace flexibility, they are also susceptible to security compromise. Mobile devices pose unique 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 when mobile devices are used.

In this audit we evaluated NASA's management of smartphones, tablets, basic cell phones, and AirCards.[1] Specifically, we assessed whether NASA had implemented controls to manage (1) the costs associated with Agency-issued mobile devices and (2) the security risks associated with personal smartphones and tablets connecting to NASA networks. Details of our audit's scope and methodology can be found in Appendix A.

Results

Weaknesses in NASA's mobile device management practices mean the Agency is unable to ensure that it is not paying for unused devices. Specifically, NASA lacks a complete and accurate inventory of Agency-issued mobile devices, which makes it difficult for the Agency to determine whether contractor charges are accurate. In addition, although NASA has taken some steps to mitigate security risks associated with personally owned mobile devices, more work remains.

NASA Lacks Accurate Inventory of Mobile Devices. NASA does not have a complete and accurate inventory of Agency-issued smartphones, tablets, cell phones, and AirCards. This occurred because the information system NASA uses to order these devices from its IT contractor is not fully functional or integrated with the database the Agency uses to track IT assets. In 2013, HP Enterprise Services, NASA's main IT contractor, reported that 2,280, or 14 percent, of Agency-issued mobile devices went unused for at least 7 months. We were unable to determine the exact cost to NASA associated with the

[1] An AirCard is a device that provides the user with access to wireless broadband cellular services.

unused devices because the information needed to match individual devices with related service charges was often missing, incomplete, or inaccurate. However, we estimate that for the 7-month period – June through December 2013 – the unused devices cost NASA more than $679,000. Until NASA resolves its asset inventory and data quality issues and strengthens controls over Agency-issued mobile devices, Agency funds will continue to be wasted on unused devices.

Despite Efforts to Address Security Vulnerabilities, More Work Remains. During the course of our audit, NASA took actions to address information security risks associated with personal mobile devices connecting to NASA's e-mail systems. Specifically, in September 2013, NASA began enforcing security requirements on all smartphones and tablets that connect to NASA's e-mail systems. However, NASA still needs to implement a technical tool to mitigate risks when those devices connect to other NASA networks apart from the e-mail systems.

Management Action

To improve management of mobile devices, we recommend that NASA's Chief Information Officer (1) develop and maintain an accurate inventory of Agency-issued mobile devices and (2) implement a third-party tool that enables centralized management of smartphones and tablets that connect to NASA networks.

In response to our draft report, NASA's Chief Information Officer concurred with our findings and recommendations and proposed corrective actions to (1) improve the Configuration Management Database so that it will more accurately track NASA-issued mobile devices and (2) implement a Mobile Device Management capability to centrally manage Agency Consolidated End-user Services-supplied, NASA-supplied, and personally owned mobile devices that connect to NASA networks. We consider the proposed actions to be responsive and will close the recommendations upon completion and verification of those actions. Management's response is reprinted in Appendix B.

CONTENTS

INTRODUCTION

Background

Mobile electronic devices, including smartphones and tablets, are key components of NASA's strategy to provide its employees flexibility in accessing Agency networks and information from anywhere at any time. Mobile computing technology enables NASA's employees and contractors to connect to the Agency's information technology (IT) infrastructure through wireless or wired networks. Beginning in July 2007, NASA began requiring that mobile devices and services be purchased through an Agency-wide contract known as the Outsourcing Desktop Initiative for NASA (ODIN). The ODIN contract was followed by the Agency Consolidated End User Services (ACES) contract with HP Enterprise Services (HP). NASA acquires most of the mobile devices and services it provides to employees through the ACES contract. In addition to Agency-owned devices, many NASA employees and contractors access NASA networks using personally owned mobile devices.

In January 2014, the Office of Inspector General (OIG) issued a memorandum to NASA management identifying concerns regarding NASA's ACES contract with HP.[2] We found that the ACES contract fell short of Agency expectations for several reasons, including a lack of technical readiness by NASA for an Agency-wide IT delivery model, unclear contract requirements, and the failure of HP to properly deliver on important aspects of the contact.

Further, in a June 2013 OIG report, we highlighted a series of challenges stemming from ineffective IT governance and shortcomings in NASA's IT security policies.[3] We reported that the decentralized nature of NASA's operations and its longstanding culture of autonomy hinder the Agency's ability to implement effective IT governance and that NASA's IT governance model weakens accountability and does not ensure that IT assets across the Agency are cost effectively managed and secure.

In addition, in a December 2012 OIG report, we found that NASA's Chief Information Officer could not fully account for the Agency's laptop computers to ensure they were encrypted and complied with applicable IT security policies.[4] We reported that NASA's efforts to install full-disk encryption on all Agency laptop computers had been repeatedly delayed due to slow implementation of the ACES contract, the highly decentralized nature of IT management at NASA, and a lack of sufficient internal controls. Moreover,

[2] NASA OIG, "Review of NASA's Agency Consolidated End-User Services Contract (IG-14-013, January 30, 2014).

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

[4] NASA OIG, "NASA's Efforts to Encrypt its Laptop Computers" (Memorandum to the Administrator, December 17, 2012).

NASA had no reliable accounting of the number of laptops in its possession and therefore was not able to ensure that encryption software was installed on 100 percent of required machines by its self-imposed deadline.

In this report, we focus on NASA's management of smartphones, tablets, and associated services.

Mobile Devices and Services at NASA. Smartphones and tablets used by NASA employees and contractors fall into one of three general categories based on ownership and management:

- *ACES-provided devices*. NASA acquires these devices and services from HP, paying the company monthly for the devices and associated services (e.g., data charges). As of June 2013, HP managed approximately 11,300 smartphones and tablets for NASA employees and contractors.
- *NASA-owned devices*. NASA purchases these devices and obtains associated data services outside of the ACES contract. As of June 2013, NASA owned and managed more than 1,500 smartphones and tablets.
- *Personal devices*. The individual user owns and pays for the device and associated services with personal funds. As of June 2013, NASA employees and contractors were accessing Agency internal network systems using more than 13,000 personal smartphones and tablets. The use of personal smartphones and tablets to access NASA information is sometimes referred to as "BYOD" or "Bring Your Own Device."

In addition to smartphones and tablets, we estimated that NASA furnishes its employees and contractors with more than 5,400 basic cell phones and AirCards.

ACES Invoices. The ACES contract requires HP to submit invoices to the NASA Shared Services Center (NSSC) on the 15 of each month for the previous 30 days of service.[5] The NSSC administers the ACES contract and pays for ACES charges using the following model:

- Base services for all users are charged to Office of the Chief Information Officer accounts. Base services include e-mail, user authentication, encryption, loaner pool management, IT security such as patch management and malware protection, emergency management, and software licenses.
- Fees for individual smartphones, tablets, cell phones, and AirCards are charged to the Center where the user is employed or a resident.

[5] The NASA Shared Services Center is a partnership between NASA and Computer Sciences Corporation. The NASA Shared Services Center consolidated selected activities from ten NASA Centers including financial management, human resources, IT, procurement, and Agency business support.

Information Security Risks Associated with Smartphones and Tablets. One of the most difficult aspects of managing mobile devices is addressing associated information security risks. Because of their portability and size, smartphones and tablets are more likely to be lost or stolen than laptops. For example, in 2011, NASA reported 146 smartphones and tablets lost or stolen compared to 45 laptops. In 2012, the numbers were 213 and 62, respectively. Moreover, smartphones are capable of storing relatively large amounts of data – in the case of ACES smartphones and tablets up to 64 gigabytes. Finally, the diversity of mobile devices and associated operating systems available also present security challenges for NASA IT officials.

NASA employees and contractors use a variety of operating systems, including:

- *BlackBerry*. BlackBerry is a proprietary system developed by Research in Motion. NASA has been providing BlackBerry smartphones to employees since 2003.
- *iOS*. iOS is a proprietary system developed by Apple for its iPhones and iPads. NASA has been providing iPhones since 2009, and both the iPhones and iPads are currently available to NASA employees and contractors through the ACES contract.
- *Android*. Google led the development of Android, an operating system for mobile devices based on the Linux operating system. Android is an "open" operating system, which means that its software code is publicly available and can be tailored to the needs of individual devices and telecommunications carriers. Accordingly, many different versions of the software are in use. Although Android devices are not available under the ACES contract, NASA owns some of these devices and some employees and contractors access NASA networks with personal devices that use the Android system.

In May 2013, the Federal Chief Information Officer Council (CIO Council) identified the top security threats posed by smartphones and tablets and suggested mitigation techniques, as shown in Table 1.[6]

[6] The Federal CIO Council, "Government Mobile and Wireless Security Baseline," May 23, 2013.

Table 1. Common Threats and Mitigations for Smartphones and Tablets

Common Threats	Mitigations
• insecure configuration • unauthorized access • virus or malware • loss of sensitive data • device loss or theft	• device management • password to unlock device • user training • encryption of data at rest • remote wipe of Agency applications and data

Source: The Federal CIO Council.

According to the Federal CIO Council, the most critical element to ensuring the security of mobile devices is effective device management, which includes configuration of the operating systems, applications, and software patches.[7] Many vendors offer third-party tools to manage the major classes of mobile devices. Using these tools, NASA can monitor for out of date or unsecure operating systems and applications.

Objectives

Given NASA's expanding use of smartphones, tablets, and other mobile computing technologies, we evaluated the Agency's management of these devices to assess (1) the costs associated with ACES-provided devices and associated mobile services and (2) the security risks associated with these devices connecting to NASA's networks. See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior coverage.

[7] The Federal CIO Council and Department of Homeland Security, "Mobile Security Reference Architecture," May 23, 2013, defines mobile device management as "any process or tool intended to manage applications, data, and configuration settings on mobile devices."

NASA NEEDS TO IMPROVE MANAGEMENT OF MOBILE DEVICES TO SAVE MONEY AND MITIGATE SECURITY RISKS

NASA does not have a complete and accurate inventory of Agency-issued smartphones, tablets, cell phones, and AirCards. This occurred because the information system NASA uses to order IT equipment from HP, its main IT contractor, is not fully functional or integrated with the database it uses to track Agency IT assets. In 2013, HP reported that 2,280, or 14 percent, of Agency-issued mobile devices went unused for at least 7 months. We were unable to determine the exact amount NASA paid for the unused devices because the information needed to match individual devices with related billings was often missing, incomplete, or inaccurate. However, we estimated that from June through December 2013 these unused devices cost NASA more than $679,000. Until NASA resolves its asset inventory and data quality issues and strengthens controls over Agency-issued mobile devices, the Agency will continue to waste funds on unused devices. We also found that while NASA has taken steps to mitigate security risks associated with personally owned smartphones and tablets accessing its e-mail systems, more work is required to reduce risks when those devices access other NASA networks.

NASA's Inability to Account for and Track Mobile Devices Means It Cannot Ensure Billings Are Accurate

Neither NASA nor HP has an accurate inventory of Agency-issued mobile devices. NASA officials admitted they had no authoritative database of these devices and were not confident that HP could accurately account for the full inventory of mobile devices it provides to the Agency. This is similar to a finding identified in our December 2012 special review where we determined that NASA did not have a full inventory of Agency-issued laptops. The lack of a complete inventory adversely affects NASA's ability to verify the accuracy and completeness of ACES invoices and leaves the Agency susceptible to paying erroneous or excessive charges.

Lack of a Comprehensive Inventory of ACES Mobile Devices. The Configuration Management Database (CMDB) NASA uses to identify, maintain, track, and report ACES managed IT equipment is not accurate and complete. Moreover, the system NASA uses to order mobile devices – the Enterprise Service Request System (ESRS) – is not integrated with the CMDB. Consequently, NASA has no automated, fully functional mechanism for tracking equipment orders and receipts, and data regarding new orders made through the ESRS must be manually uploaded into the CMDB. On the billing side, HP provides NASA an itemized monthly invoice on the 15 of each month containing information for each ACES services, including the user name, location, associated asset

tag, and itemized charge for each type of service. HP also provides a monthly Agency Cellular Seat Detail Report of the minutes and data used by each device.

If ESRS and CMDB were integrated, the CMDB would automatically populate with complete data concerning the mobile devices for which the Agency is paying. Instead, since the start of the ACES contract in November 2011, NASA officials have been manually populating the CMDB with data from Excel spreadsheets supplied by HP. Compounding the problem are questions about the accuracy of the data provided by HP. For example, in July 2013, NASA "scrubbed" the CMDB database and removed almost 40,000 erroneous records. During our review, we could not accurately reconcile data from the Agency Cellular Seat Detail Reports to the HP monthly billing invoices due to missing inventory control numbers.

Thousands of ACES Mobile Devices Unused. We estimate that from June through December 2013, NASA had 2,280 mobile devices that were not used and cost more than $679,000 over the 7-month period, of which 47% of these costs can be attributed to smartphones. We could not determine the actual amount paid by NASA for these devices because information needed to link individual devices with monthly billing statements was missing, incomplete, or inaccurate. Mobile device accounts in the Agency Cellular Seat Detail Reports did not have unique identifiers needed to match devices with corresponding invoices. Accordingly, we estimated the amount of potential mischarges by multiplying the average monthly cost for each type of device by the number of unused devices and applying that amount over the months the devices went unused. Because our estimate did not include charges for optional services such as international data plans, the $679,000 estimate may actually understate the amount NASA paid for these unused mobile devices. Table 2 shows the type, number, and estimated costs associated with unused mobile devices at NASA for the period June to December 2013.

Table 2. Estimated Costs for Unused Mobile Devices or Services

Mobile Device	Unused for 7 Months (June through December 2013	Estimated Total for June 2013	Unused (as a Percentage of Estimated Total for June 2013)	Cost[a]
AirCard	990	2,950	34%	
Cell Phones	470	2,430	19%	
Smartphones	760	10,450	7%	
Tablets	60	870	7%	
Total	**2,280**	**16,700**	**14%**	**$679,980**

[a] The individual cost for each type of device is proprietary information and has been redacted.

Source: OIG analysis of Agency Cellular Detail Reports for June through December 2013.

NASA officials are working to better integrate the CMDB and ESRS systems and recently formed a task force to address implementation issues and identify authoritative sources of data. Once the database becomes more reliable, the NSSC contractor (Computer Sciences Corporation) will use the system to validate the accuracy of invoices submitted by HP. Although NASA has taken interim action to review invoices and has rejected those found to have errors, the Agency still primarily relies on the individual organizations at the Centers to identify appropriate charges for its mobile devices.

Moreover, included in NASA's ACES contract modification dated October 24, 2013, is an agreement between HP and NASA that states "[HP] will forgo billing for any unordered Mobility Lines and unused Mobility Lines for the period November 1, 2011 through May 2013…" While this modification indicates that NASA is not required to pay for unused and unordered lines, we have serious doubts regarding how well NASA or HP is able to identify the population of unused devices going back 2 years or into the future without an accurate inventory.

NASA Addresses Some Security Vulnerabilities But More Remain

At the time we initiated this audit, we found that NASA had not addressed serious information security risks associated with employees and contractors using personal smartphones and tablets to access NASA networks, including the potential for unauthorized access if these devices were lost or stolen. In September 2013, NASA took corrective actions and now enforces security requirements on all smartphones and tablets that connect to NASA's e-mail systems, whether the devices are ACES-provided, NASA-owned, or personal equipment. Specifically, NASA requires all mobile devices that connect to its e-mail systems to have a password, automatic lock after a period of inactivity, native encryption, and be configured to automatically delete all data after 10 failed password attempts.[8]

Through these new requirements, NASA has mitigated several major security risks; however, more work remains to mitigate risks associated with mobile devices connecting to other NASA networks, such as local area networks at each of the Centers.

Security Requirements for Access to NASA E-mail Systems. Prior to September 2013, NASA enforced security controls – including minimum hardware requirements, a password requirement of at least four characters, automatic lock after a period of inactivity, use of native encryption from the device, and automatic deletion of all data on the device after 10 failed password attempts – on Agency-issued equipment. However, similar controls were not in place for all personal devices that connected to NASA networks.

In November 2012, NASA established the Mobile Security Focus Group to develop security requirements to support the Agency's plan to "securely and seamlessly access

[8] Native encryption refers to the data at rest encryption provided by the mobile device itself and is different from the Entrust product that NASA uses to encrypt documents and e-mails.

and share any information, anyplace, anytime, using any device."[9] In June 2013, the Mobile Security Focus Group identified an immediate need to enforce security requirements on personal devices accessing NASA's e-mail systems. Consequently, as of September 2013, all devices that connect to NASA's e-mail systems were required to have a password of at least four characters, automatically lock after a period of inactivity, use encryption, and automatically delete all data on the device after 10 failed password attempts.[10, 11] We believe this is a positive step toward better management of the information security risks associated with mobile devices accessing NASA's e-mail systems.

Remaining Work to Mitigate Security Risks. Nevertheless, more work remains to mitigate risks associated with mobile devices that connect to NASA's non-e-mail systems and networks, such as the wireless local area networks at the NASA Centers. In April 2013, NASA's Office of the Chief Information Officer established the Mobile Device Management Integrated Product Team to identify requirements for a third-party tool that would enable the Agency to perform centralized mobile device management. Such a tool would provide configuration management of mobile devices that connect to NASA's wireless network and help NASA manage risks from devices that would otherwise have unsecure configuration.

The National Institute of Standards and Technology identified third-party tools as a technical solution for controlling the use of both organization-furnished and personal mobile devices. Without these tools, NASA would need to manage mobile devices individually and manually, which poses two major security problems.

1. The security controls provided by an individual's mobile device often lack the rigor of those provided by a centralized organization. For example, a personal mobile device may only support a short passcode for authentication and may not support strong data encryption.
2. It will require significantly more effort or may not be possible to manage the security of the device when it is not physically present within the enterprise.

[9] The IT Management Board consists of the Agency CIO, the Deputy and Associate CIOs, the Center CIOs, and the Mission Directorate CIOs and makes decisions regarding the Agency's IT infrastructure strategy, operations, and budget. The IT Management Board is a forum for oversight and evaluation of Agency IT operations and maintenance and for reviewing and approving high-level requirements of critical infrastructure initiatives. The NASA CIO serves as the decision authority for the IT Management Board.

[10] The Mobile Security Focus Group was led by the IT Security Division of NASA's Office of the Chief Information Officer and included members from Ames Research Center, Kennedy Space Center, and Marshall Space Flight Center.

[11] The Memorandum from the NASA Chief Information Officer, "Minimum Security Requirements for Personal Mobile Devices," August 27, 2013, provides a list of security requirements for the use of personal devices.

Conclusion

NASA faces challenges with implementing a cost-effective and secure mobile computing strategy. The Agency needs a comprehensive and accurate inventory to more effectively manage its mobile assets. Without such a system, NASA will continue to expend significant resources to validate the accuracy of monthly invoices provided by HP. In addition, without an accurate inventory the Agency will continue to pay erroneous or excessive charges on unused devices.

In September 2013, the Agency implemented security controls to mitigate risks from personal smartphones and tablets connecting to its e-mail infrastructure. In addition, NASA initiated work to identify an Agency third-party tool to manage mobile devices. While these initiatives are positive steps, NASA remains vulnerable to information security risks associated with smartphones and tablets until these new systems are fully implemented.

Recommendations, Management's Response, and Evaluation of Management's Response

To help improve the management and security of its mobile devices, we made the following recommendations to the NASA Chief Information Officer (CIO):

Recommendation 1. Develop and maintain an accurate inventory of Agency-issued mobile devices.

Management's Response. The CIO concurred with our recommendation, stating that his office is taking action to improve the Configuration Management Data Base so that it will more accurately track Agency-issued mobile devices. In addition, he indicated that the OCIO has established a project team to identify and address the business architecture, systems, and processes associated with management and invoicing of mobile devices. The CIO estimated completion of these actions by August 30, 2014.

Evaluation of Management's Response. Management's proposed actions are responsive to our recommendation. Therefore, we consider the recommendation resolved and will close it upon receipt and verification of those actions.

Recommendation 2. Implement a third-party tool or tools that would enable the Agency to centrally manage personally owned smartphones and tablets that connect to NASA networks.

Management's Response. The CIO concurred with our recommendation, stating that his office is implementing an enterprise Mobile Device Management capability that will address management of ACES supplied/managed devices, non-ACES supplied devices (Government Furnished Equipment), and personally owned

equipment (Bring Your Own Devices). The CIO estimated completion of this action by February 28, 2015.

Evaluation of Management's Response. Management's proposed action is responsive to our recommendation. Therefore, we consider the recommendation resolved and will close it upon receipt and verification of the action.

SCOPE AND METHODOLOGY

We performed this audit from June through July 2012, and from October 2012 through February 2014 in accordance with generally accepted government auditing standards.[12] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our review of controls to manage the security risks did not include laptops because the security controls available for laptops are quite different from those available for smartphones, tablets, and other mobile device types. Mobile devices with minimal computing capability, such as the most basic cell phones, are also out of the scope of the security review because of the limited security options available and the limited threats they pose. In addition, tablets were limited to those running mobile operating systems and did not include laptops in tablet form, such as Microsoft Surface Pro.

We interviewed NASA Headquarters and Center officials, the Enterprise Service Desk Service Manager, NSSC IT Infrastructure Integration Program Business Office officials, the Enterprise Service and Integration Division, Service Integration Manager, and ACES Subject Matter Experts concerning mobile security, inventory controls, and mobile device ordering and receiving process. We reviewed the ACES contract to obtain an understanding of the pricing and services for mobile devices. We analyzed the monthly Agency Cellular Seat Detail Reports for June through December 2013 for devices that were unused for the 7-month period.

Federal Laws, Regulations, Policies, and Guidance. We reviewed the following in the course of our audit work:

- Executive Order 13589, "Promoting Efficient Spending," November 2011
- National Institute of Standards and Technology Special Publication 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013
- NASA Procedural Requirements 1382.1.A, "NASA Privacy Procedural," August 10, 2007

[12] The audit was temporarily suspended from August 1, 2012, through October 29, 2012, to complete other audit priorities.

- NASA Procedural Requirements 2810.1A, "Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)," May 16, 2006
- NASA Technical Standard NASA-STD-2805P, "Minimum Hardware Configuration," amended April 8, 2013
- NASA IT Security Handbook ITS-HBK-2810.15-01A, "Access Control," September 4, 2012
- Memorandum from the NASA Chief Information Officer, "Minimum Security Requirements for Personal Mobile Devices," August 27, 2013
- GAO/AIMD-00-21.3.1, "Standards for Internal Control in the Federal Government," November 1999

Use of Computer-Processed Data. We used computer-processed data from the NASA Property System to perform this audit. We obtained data from the system as of June 5, 2013, to identify the number of government-owned smartphones and tablets. We also used computer-processed data from HP Enterprises Service and ACES Portal. We found this data to be unreliable; specifically, the data was not complete, accurate, or consistent. As a result, we were unable to quantify potential costs savings in our findings or conclusions.

Review of Internal Controls

We reviewed internal controls related to the oversight of ACES devices and security of smartphones and tablets connecting to NASA's e-mail systems. This included determining whether NASA has policies and procedures in place specific to personal devices.

Prior Coverage

During the last 5 years, the NASA OIG and the Government Accountability Office (GAO) have issued four reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at http://oig.nasa.gov/audits/reports/FY14/index (NASA OIG) and http://www.gao.gov (GAO).

NASA Office of Inspector General

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

"NASA's Efforts to Encrypt its Laptop Computers" (Memorandum to the Administrator, December 17, 2012)

Government Accountability Office

"Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged" (GAO-12-757, September 18, 2012)

"Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks" (GAO-10-3SU, October 15, 2009)

MANAGEMENT COMMENTS

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

FEB 27 2014

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Response to OIG Draft Report Entitled "NASA's Management of Its Smartphones, Tablets, and Other Mobile Devices" (A-12-023-00)

NASA appreciates the opportunity to review your draft report entitled "NASA's Management of Its Smartphones, Tablets, and Other Mobile Devices" (A-12-023-00).

In the draft report the Office of Inspector General (OIG) cites the lack of a complete and accurate inventory of Agency-issued mobile devices, which makes it difficult for NASA to determine whether contractor charges are accurate. In addition, although NASA has taken some steps to mitigate security risks associated with personally owned mobile devices, more work remains to mitigate related security risks. The OIG makes two recommendations, addressed to the Chief Information Officer, to help improve the management and security of its mobile devices. NASA's response to the recommendations, including the schedule for planned corrective actions, follows:

Recommendation 1: Develop and maintain an accurate inventory of Agency-issued mobile devices.

Management's Response: Concur. The Office of the Chief Information Officer (OCIO) is taking corrective actions to address issues with the Configuration Management Data Base (CMDB) which will be used to track Agency-issued mobile devices. Currently, the OCIO and Centers are validating the assignment and invoicing of all mobile assets. Additionally, the OCIO has established a project team to identify and address the business architecture, systems, and processes associated with the management and invoicing of mobile devices.

Estimated completion date: August 30, 2014.
Milestones:

- March 2014: Agency-issued Mobile device reconciliation with Agency Consolidated End-User Services Contract (ACES) invoices
- April 2014: CMDB updated to manage and track ACES issued mobile devices
- August 2014: Management of non-ACES mobile devices implemented using CMDB of local Center asset management systems

Recommendation 2: Implement a third-party tool or tools that would enable the Agency to centrally manage personally owned smartphones and tablets that connect to NASA networks.

Management's Response: Concur. The OCIO is implementing an enterprise Mobile Device Management (MDM) capability. A project team has been established. The project will be composed of three phases of implementation addressing the management of: 1) ACES Supplied/Managed devices; 2) Non-ACES supplied devices (Government Furnished Equipment); and 3) Personal (Bring-Your-Own-Devices).

Estimated completion date: February 28, 2015.

Milestones:

- September 2014: MDM implementation for ACES Supplied/Managed Devices
- December 2014: MDM implementation for non-ACES Supplied/Managed Devices
- February 2015: MDM support for Personal (BYOD) Devices

We have reviewed the draft report for information that we believe should not be publicly released and have provided our concerns regarding public release of that information to the OIG.

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 Gretchen Davidian at (202) 358-0831.

Larry N. Sweet

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Associate Administrator
Chief of Staff
Chief Information Officer
Chief Scientist

Non-NASA Organizations and Individuals

Office of Management and Budget
    Deputy Associate Director, Energy and Science Division
        Branch Chief, Science and Space Programs Branch
Government Accountability Office
    Director, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
    Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
    Subcommittee on Science and Space
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
    Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Oversight and Government Reform
    Subcommittee on Government Operations
House Committee on Science, Space, and Technology
    Subcommittee on Oversight
    Subcommittee on Space

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate
Mindy Vuong, Project Manager
Deirdre Beal, Auditor
Howard Kwok, Auditor
Christopher Reeves, Information Technology Specialist

FEBRUARY 27, 2014

REPORT No. IG-14-015

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY14/ to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

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