OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices

Report No.: 2015-ITA-032

June 2016

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

JUN 22 2016

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall
Deputy Inspector General

Subject: Final Audit Report – U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices
Report No. 2015-ITA-032

This report transmits the results of our audit of mobile computing device management. We reviewed whether the U.S. Department of the Interior (DOI) effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limiting the number of mobile computing devices issued, and monitoring usage to ensure public funds are not spent on unused mobile devices. We also assessed the adequacy of DOI's implemented controls to mitigate security risks unique to mobile computing devices.

We identified weaknesses in DOI's mobile device management practices that have resulted in DOI spending tens of thousands of dollars on unused mobile devices. We found that DOI did not have a complete inventory of its mobile devices and services and did not implement a Departmentwide approach for procuring and managing these devices. In addition, we found that some of DOI's mobile computing devices do not have proper security configurations, which could result in unauthorized access to Government systems and data by cybercriminals.

We offered four recommendations to help DOI improve its management and security of mobile computing devices. In its response to our draft report, the Office of the Chief Information Officer (OCIO) concurred with two recommendations and did not concur with two recommendations (see Appendix 3). Based on OCIO's response, we consider three recommendations resolved but unimplemented and one recommendation unresolved (see Appendix 4). We will refer all four recommendations to the Office of Policy, Management and Budget to track their implementation and resolution.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief

Mobile computing devices, such as smartphones and tablets, are key components of the U.S. Department of the Interior's (DOI) information technology (IT) strategy. These devices allow employees access to DOI data and systems from anywhere at any time, as well as the ability to store large amounts of data. DOI spends approximately $16.5 million each year on at least 35,576 mobile devices. The benefits mobile devices afford, however, can also be the greatest risk. Because they are small, hand-held, and portable, mobile devices that are not physically secured by the user are highly vulnerable to theft, loss, and damage

We found that DOI did not have a complete inventory of its mobile devices and services and did not implement a Departmentwide approach for procuring and managing these devices. As a result, DOI has spent hundreds of thousands of dollars on unused mobile devices. We reviewed mobile usage and inventory data for the four DOI bureaus that had the most Government-issued mobile devices: Bureau of Land Management (BLM), National Park Service (NPS), U.S. Fish and Wildlife Services (FWS), and U.S. Geological Survey (USGS). As a result of our analysis of usage data from October 1, 2014, to March 30, 2015, we found that the four bureaus spent $50,470 a month on 1,557 unused mobile devices.

In addition, we found that thousands of DOI's mobile computing devices do not have proper security configurations, which could result in unauthorized access to Government systems and data by cybercriminals. The National Institute of Standards and Technology recommended that organizations enroll mobile devices in an enterprise-wide management solution to ensure required security controls and usage policies are implemented on the devices before they are issued to employees.[1] As of June 2015, we found that DOI had not enrolled thousands of devices issued by the four bureaus in the Departmentwide mobile device management solution. This deficiency could result in potential security breaches, as these devices are vulnerable to unauthorized access by cybercriminals.

As DOI employees increasingly rely on tablet computers and smartphones to perform their jobs, it is imperative that DOI improve the inventory, acquisition, issuance, use, monitoring, and securing of its mobile computing devices. Full implementation of our recommendations by DOI's Chief Information Officer will help DOI improve its management and security of mobile computing devices.

[1] An enterprise-wide management solution is one that encompasses centralized management of mobile devices across the entire organization as a whole rather than having each office or department separately manage its devices.

Introduction

Objective

We reviewed mobile computing device management at the U.S. Department of the Interior (DOI) to determine whether DOI effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limiting the number of mobile computing devices issued, and monitoring usage to ensure public funds are not spent on unused mobile devices. We also assessed the adequacy of DOI's implemented controls to mitigate security risks unique to mobile computing devices. Appendix 1 provides further details of our scope and methodology.

Background

According to the U.S. Government Accountability Office (GAO), Federal agencies spend about $1.2 billion annually on mobile computing devices and services. Mobile computing devices are key components of the Government's information technology (IT) strategy, offering employees the flexibility to access systems and data from anywhere at any time. The U.S. Office of Management and Budget (OMB) requires Federal agencies to use an enterprise-wide approach for procuring and managing mobile computing devices to reduce costs and improve the ability to track mobile device usage, secure devices, and deliver mobile applications.[2] Federal agencies are also required to maintain mobile device inventories, monitor usage, and establish controls to ensure that public funds are not spent on unused or underutilized mobile devices.[3]

While mobile devices with computing capabilities[4] offer greater workplace flexibility, these devices are also susceptible to security compromise because of their size, portability, constant wireless connection, physical sensors, and location services. Moreover, the diversity of available devices, operating systems, carrier-provided services, and applications used on the devices present additional security challenges. Finally, despite their small size, mobile devices can store large amounts of data.

The Federal Chief Information Officer Council identified the top security threats for mobile devices and suggested mitigation strategies (see Figure 1). [5] The Council recommended that Federal agencies implement an enterprise-wide mobile device management solution that allows users to securely access Government resources while protecting the services and data accessed.

[2] "Digital Government: Building A 21st Century Platform To Better Serve The American People," OMB, May 23, 2012.
[3] Executive Order 134589, "Promoting Efficient Spending," November 2011.
[4] Mobile devices with computing capabilities refer to smartphones and tablet computers.
[5] The Federal Chief Information Officer Council and U.S. Department of Homeland Security, "Mobile Security Reference Architecture," May 23, 2013.

Common Threats	Mitigation Strategies
• Insecure configuration • Unauthorized access • Virus and malware • Loss of sensitive data • Device loss or theft	• Device management • Password to unlock device • User training • Encryption of data • Remote wipe of DOI applications and data

Figure 1. Common Threats and Mitigation Strategies for mobile devices.
Source: The Federal Chief Information Officer Council and U.S. Department of Homeland Security, "Mobile Security Reference Architecture," May 23, 2013.

DOI's Use of Mobile Devices

DOI spends about $16.5 million annually on approximately 35,576 mobile computing devices, including smartphones and tablet computers. DOI's mobile devices can store large amounts of data, despite their small size, with storage capabilities of up to 32 gigabytes for smartphones and up to 64 gigabytes for tablets.

DOI employees and contractors are approved to use two different operating systems:

- **Android:** Android is a Linux-based operating system developed by Google for mobile phones and tablets. The open-source nature of Linux allows individual users to tailor this operating system to meet his or her needs, which provides varying security risks.
- **iOS:** Apple developed iOS as the operating system for its iPhones and iPads.

To effectively secure and remotely manage its portfolio of mobile devices, DOI's Office of the Chief Information Officer (OCIO) selected MaaS360 as its mobile device management solution. MaaS360 is a commercial device management platform that can ensure devices have security configurations that are in compliance with DOI's IT security policy.[6]

At the time of our audit, GAO conducted a Governmentwide review of mobile device management practices. GAO's review included the U.S. Fish and Wildlife Service (FWS) and the National Park Service (NPS). GAO issued a report in May 2015, offering three recommendations to help DOI effectively manage spending on mobile devices and services.[7] GAO recommended that DOI:

[6] U.S. Department of the Interior OCIO Memorandums, "Risk Acceptance for the Use of Apple iPads, iPhones, iOS 5, and iTunes Desktop/Laptop Application Suite," June 7, 2012; and "Risk Assessment for Google Android Operating System and Android Hardware," November 16, 2012.
[7] "Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services," GAO-15-431, May 2015.

1) ensure an inventory of mobile devices and services is established Departmentwide (i.e., all components' devices and associated services are accounted for);
2) ensure a reliable Departmentwide inventory of mobile service contracts is developed and maintained; and
3) ensure procedures to monitor and control spending are established Departmentwide. Specifically, ensure that—
    i. procedures include assessing devices for zero, under, and over usage;
    ii. personnel with authority and responsibility for performing the procedures are identified; and
    iii. the specific steps to be taken to perform the process are documented.

DOI concurred with GAO's recommendations, and DOI's written response included planned actions to address each recommendation. Some of our findings related to inventory management and device usage are similar to GAO's. Therefore, we did not make recommendations that duplicate those already made. Our audit, however, also quantified overspending by DOI on unused mobile devices and included IT security findings.

Findings

As the use of mobile devices to conduct daily operations continues to increase, DOI must improve its governance and security controls over mobile devices in order to recognize cost savings and bolster IT security. We found that DOI spends approximately $600,000 a year on unused mobile devices at the four bureaus we reviewed: Bureau of Land Management (BLM), U.S. Geological Survey (USGS), FWS, and National Park Service (NPS), U.S. Fish and Wildlife Service (FWS), and U.S. Geological Survey (USGS). Moreover, DOI's decentralized approach for purchasing mobile devices and services is inefficient and hinders DOI from reducing costs by leveraging its buying power with service providers.

Furthermore, we found that thousands of mobile devices did not have the security configurations installed as mandated by the OCIO, which could result in unauthorized access to Government data, especially if these devices are lost or stolen. In addition, if a cybercriminal accesses an unsecure mobile device, the criminal could use data on the device to gain unauthorized access to DOI networks and systems. We believe these deficiencies occurred because DOI did not—

1. maintain an inventory of its mobile devices and had not developed or implemented effective policies and procedures to govern the acquisition, issuance, use, and monitoring of mobile devices and services; and
2. enroll mobile devices in its mobile device management solution to ensure the required security controls and usage polices had been implemented before issuing the devices to employees.

Bureau Spending on Unused Mobile Devices Exceeds $600,000 Annually

Executive Order requires Federal agencies to maintain inventories, monitor device usage, and establish controls to ensure that public funds are not spent on unused or underutilized mobile devices.[8] We analyzed Verizon usage data from October 1, 2014, to March 30, 2015—the most recent time period that usage data were available—and found that BLM, FWS, NPS, and USGS spent $50,470 per month (for 1 or more months) on 1,557 unused mobile devices (see Figure 2), resulting in approximately $600,000 per year. Assuming that the bureaus continue with the current cellular plans for the next 3 years, spending on unused mobile devices would exceed $1.7 million based on the 3-year discount rate established by the Office of Management and Budget (see Appendix 2).

We also identified 486 activated mobile devices at the four bureaus that had zero usage for the 3-month period that ended September 2014 (see Figure 3). Prolonged periods of zero usage may indicate that the bureaus issued mobile

[8] Executive Order 134589, "Promoting Efficient Spending," November 2011.

devices to employees without a valid business need or that devices were lost or stolen but unreported.

Bureau	Unused Mobile Devices as of March 2015	Total Plan Amount
BLM	803	$16,049
FWS	213	$9,874
NPS	381	$17,513
USGS	160	$7,034
Total	**1,557**	**$50,470**

Figure 2. Unused Verizon mobile devices as of March 30, 2015.
Source: OIG Analysis of Verizon Wireless data provided by DOI.

Bureau	Unused Mobile Devices since 2014
BLM	116
FWS	108
NPS	184
USGS	78
Total	**486**

Figure 3. Devices that have not been used since the 3-month period that ended September 2014.
Source: OIG Analysis of Verizon Wireless data provided by DOI.

Based on the scope of our review, which included only four bureaus and only devices using Verizon as the service provider, we believe that the amount of overspending and number of unused devices Departmentwide is certainly higher. We did not have access to comparable data from DOI's other wireless service providers.[9] We also could not determine the total percentage of mobile devices and related services supplied by Verizon because not all of the four bureaus we reviewed maintained a complete inventory of mobile devices and related service plans.

We believe that expenditures on unused mobile devices occurred because the four bureaus we reviewed did not maintain an inventory of their mobile devices and had not developed or implemented effective policies and procedures to govern the acquisition, issuance, use, and monitoring of mobile devices and services. For example, the bureaus did not monitor usage to determine whether employees had a continuing business need for mobile devices. Moreover, DOI did not implement an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices as required by OMB. Instead, we found that program managers procure and manage devices locally. As a result, DOI may waste

[9] In addition to Verizon, DOI also uses AT&T, Sprint/Nextel, T-Mobile, and U.S. Cellular as wireless service providers.

Government funds on unused mobile devices. Until DOI implements measures to more effectively manage its mobile devices, it is likely that public funds will continue to be misspent on unused mobile devices.

Recommendations

We recommend that DOI:

1. Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services; and

2. Implement an enterprise-wide approach for procuring and managing DOI mobile devices.

Inadequate Enforcement of Required Security Controls Puts Sensitive Data on Thousands of Mobile Computing Devices at High Risk of Loss

Forty-one percent of data breaches result from the loss of mobile computing devices, so it is imperative to have adequate security controls to help protect the sensitive data stored on these devices.[10] To effectively secure and remotely manage its portfolio of mobile devices, DOI's OCIO selected MaaS360 as its mobile device management solution. MaaS360 is a commercial device management platform that can remotely apply and manage security configurations. In addition to secure configurations, MaaS360 also provides device encryption, secure password settings, and the ability to remotely locate, lock, and delete all data on lost or stolen mobile devices. Although MaaS360 is a Departmentwide requirement, each bureau or office must ensure that its mobile devices comply with DOI's IT security policy.[11]

In addition, the National Institute of Standards and Technology recommended that organizations enroll devices in an enterprise-wide device management solution (e.g., MaaS360) to ensure required security controls and usage polices were implemented before issuing the devices to employees.[12]

As of June 2015, we found that MaaS360 did not manage thousands of mobile computing devices issued by the four bureaus (see Figure 4). Our analysis did not include flip phones, as these devices do not have computing capabilities.

[10] TrendMicro Inc., "Follow the Data: Dissecting Data Breaches and Debunking the Myths," September 22, 2015.
[11] U.S. Department of the Interior OCIO Memorandums, "Mandatory Deployment of the Department of the Interior Enterprise System for All Bureaus and Offices," March 15, 2012; "Risk Acceptance for the Use of Apple iPads, iPhones, iOS 5, and iTunes Desktop/Laptop Application Suite," June 7, 2012; and "Risk Assessment for Google Android Operating System and Android Hardware," November 16, 2012.
[12] National Institute of Standards and Technology Special Publication SP-800-124 Rev. 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013.

Bureau	Smart-phones	Tablets	Smart-phones and Tablets	Smartphones and Tablets Managed by MaaS360	Percent Managed by MaaS360
BLM	2,533	883	3,416	2,630	77%
FWS	2,505	235	2,740	2,096	77%
NPS	3,801	585	4,386	2,716	62%
USGS	2,085	118	2,203	1,298	59%
Total	**10,924**	**1,821**	**12,745**	**8,740**	**69%**

Figure 4. Verizon mobile computing devices used by the four bureaus managed by MaaS360 as of June 2015.
Source: OIG Analysis of Verizon Wireless data provided by DOI.

Devices not managed by MaaS360 can still be used to login to any DOI system that is accessible over the Internet from a web browser. This includes Gmail and related Google applications (e.g., Google Drive, Google Documents, etc.). In addition, device users may potentially download gigabytes of information from DOI systems, including files with sensitive data, to their unencrypted smartphones or tablets. As such, we found that the absence of required security controls potentially compromises thousands of DOI mobile devices to unauthorized access if the devices are lost or stolen. Further, the extent of the potential security breach is not limited to the compromised mobile device. For example, a cybercriminal in control of an unprotected mobile device could potentially use information on it (e.g., user names and passwords) to gain unauthorized access to DOI's computer networks and systems.

The loss or theft of a mobile computing device is a security incident that is recorded in a Departmentwide incident tracking system. Unfortunately, because the system has limited reporting capabilities, we were unable to determine the number of lost or stolen mobile computing devices that may put sensitive Government data at risk to unauthorized access.

We found that the four bureaus did not follow the recommended best practice of enrolling mobile devices in MaaS360 before issuing the devices to employees. Instead, the bureaus issued activated and fully functional smartphones and tablet computers to employees along with instructions for how to enroll the device in MaaS360 and enable key security controls (e.g., data encryption, strong passwords, location services etc.). The bureaus did not verify if employees had enrolled their Government-issued mobile devices in MaaS360 to comply with OCIO's security policy. Therefore, thousands of DOI mobile devices are not adequately secured or centrally managed.

We believe the total number of mobile computing devices Departmentwide without the required security controls is higher than reported because our analysis included only four bureaus and was limited to mobile devices with a Verizon

Wireless service plan. In addition, our analysis did not include tablet computers that did not have a separate wireless plan and instead access the Internet using a WiFi connection.

Unless DOI improves its practices for managing security controls on its mobile devices, sensitive data on thousands of unencrypted DOI mobile devices will remain at high risk of unauthorized access.

Recommendations

We recommend that DOI:

3. Verify that its mobile device management solution (e.g., MaaS360) manages all mobile devices distributed to employees and contractors; and

4. Enroll newly acquired mobile devices in to DOI's mobile device management solution before issuing the devices to individual users.

Conclusion and Recommendations

Conclusion

DOI faces a significant challenge to implement enterprise-wide mobile device management practices. Without a complete inventory of mobile devices and services and a Departmentwide approach for procuring these devices, DOI will continue to pay for unused mobile devices and will be unable to ensure that all mobile devices are adequately secure. Further, DOI must enroll these devices in its mobile device management solution (e.g., MaaS360) to help protect against unauthorized access. As the use of mobile computing technologies expands and becomes more advanced, DOI must continually strengthen its governance and risk management practices to prevent the misuse of Government funds and help mitigate adverse effects if these devices are lost or stolen.

Recommendations Summary

We recommend that DOI:

1. Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services.

   OCIO Response: In its response to our draft report, OCIO concurred with this recommendation. OCIO stated that efforts are underway to resolve and implement the recommendations GAO made in May 2015.

   OIG Comment: Based on OCIO's response, we consider this recommendation resolved but unimplemented until OCIO satisfactorily addresses all three pre-existing GAO recommendations. We will refer this recommendation to the Office of Policy, Management and Budget (PMB) to track implementation.

2. Implement an enterprise-wide approach for procuring and managing DOI mobile devices.

   OCIO Response: OCIO concurred with this recommendation, stating that efforts are underway, through contract action and associated policies and procedures, to implement the recommendation.

   OIG Comment: Based on OCIO's response, we consider this recommendation resolved but unimplemented. We will refer this recommendation to PMB to track implementation.

3. Verify that DOI's mobile device management solution (e.g., MaaS360) manages all mobile devices distributed to employees and contractors.

   OCIO Response: OCIO did not concur with this recommendation, stating that not all mobile devices are candidates for enrollment in DOI's mobile device management solution. OCIO stated that certain mobile devices, which are not data-consumption devices, cannot be managed using the mobile device management solution and are managed using DOI's standard client management tools.

   OIG Comment: Our reference to mobile devices in the report chapter and related recommendation pertains to mobile devices with computing capabilities (e.g., smartphones and tablet computers) and not to mobile devices that provide only cellular telecommunication services (e.g., flip phones). We recognize that flip phones are not data-consumption devices and thus cannot be managed using DOI's mobile device management solution. We reiterate that departmental policy requires all iPhone, iPad, and android devices provided by DOI and connecting to DOI's network to be managed using MaaS360, DOI's enterprise-wide solution for mobile device management. Moreover, departmental policy does not mention any other approved mobile device management solutions besides MaaS360. Based on OCIO's response, we consider this recommendation unresolved. We will refer this recommendation to PMB for resolution.

4. Enroll newly acquired mobile devices in to DOI's mobile device management solution before issuing the devices to individual users.

   OCIO Response: OCIO did not concur with this recommendation, stating that not all mobile devices are candidates for enrollment in the mobile device management solution. OCIO stated, however, that DOI will issue a clarifying directive that mobile devices that process DOI data must be secured in accordance with the National Institute of Standards and Technology Special Publication SP 800-124 Revision 1 within 72 hours of being issued to individual users.

   OIG Comment: Our reference to mobile devices in the report chapter and related recommendation pertains to mobile devices with computing capabilities (e.g., smartphones and tablet computers) and not to mobile devices that provide only cellular telecommunication services (e.g., flip phones). We recognize that flip phones are not data-consumption devices and cannot be managed using DOI's mobile device management solution. As such, we consider OCIO's planned actions responsive to our recommendation. We consider the recommendation resolved but unimplemented and will refer it to PMB to track implementation.

Appendix 1: Scope and Methodology

Scope

We focused on determining whether the U.S. Department of the Interior (DOI) effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limited the number of mobile computing devices issued, and monitored device usage to ensure public funds were not spent on unused and underutilized mobile devices. We also assessed internal controls related to the security of DOI's mobile computing devices. We reviewed DOI and bureau policies, procedures, and practices for management of mobile devices throughout their lifecycle, mobile usage patterns, and device inventories. We reviewed mobile usage and inventory data for the four bureaus that issued the most mobile devices: Bureau of Land Management, National Park Service, U.S. Fish and Wildlife Service, and U.S. Geological Survey.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Methodology

DOI does not have a complete and accurate inventory of all mobile devices; therefore, to determine whether DOI effectively managed mobile devices, we requested and obtained from DOI third-party usage data for DOI's main mobile device provider, Verizon Wireless, which according to the DOI Contracting Officer, accounts for approximately 80 percent of all DOI spending on mobile devices and services. Using the Verizon Wireless usage data for October 1, 2014, through March 31, 2015, we analyzed the usage of mobile devices to determine the number, percentage, and cost of various devices with zero usage in voice or data. We traced the unused mobile devices to usage data that covered the 3 months ended September 30, 2014, and identified the activated mobile devices at the four bureaus that had zero usage for extended periods. In addition, we compared this data to the inventories of all devices that are managed in DOI's mobile device management solution in the same time period to determine whether all mobile devices managed by DOI are included in the mobile device management solution and therefore have the security controls in place required by the Office of the Chief Information Officer (OCIO).

To accomplish our objectives, we reviewed relevant Federal laws and regulations; DOI, bureau, and office policies and procedures; information related to lifecycle management of mobile devices from the bureaus and offices; usage data from vendors; and enrollment data in DOI's mobile device management solution; and

interviewed management and responsible officials from OCIO and the bureaus to understand the nature of the mobile device solution and controls implemented.

We used computer-processed data from the third-party provider, Verizon Wireless. We reviewed the Verizon usage data from October 1, 2014, through March 31, 2015. To assess the completeness and accuracy of this data, we compared the inventory listing of DOI Office of Inspector General (OIG) employees to the Verizon data and ensured that the OIG employees were included in the Verizon dataset for this time period. We chose OIG because we could verify the completeness and accuracy of OIG's inventory due to our familiarity with the office, because it centrally procures mobile devices, and because it maintains a complete and accurate inventory.

Appendix 2: Monetary Impact

We found that the U.S. Department of the Interior (DOI) spent at least $600,000 a year on unused mobile computing devices as of March 2015. The following table summarizes our estimate of potential savings DOI could realize over the next 3 years through more effective management of its mobile computing devices.

After we sent the Notifications of Potential Findings and Recommendations—which are usually issued before the audit work is completed and when some or all of the critical elements of a finding still require development—to the related bureaus, OCIO raised concerns, which it reiterated in its response to our draft report (see Appendix 3). Specifically, OCIO stated that our calculation of overspending on unused devices in our preliminary findings included lines of service that were not associated with DOI. Before issuing our draft report, we reviewed each record in the Verizon data set and excluded those records that were not associated with a DOI bureau or office. The overspending amounts we provided in the draft and final reports were based on the data set from which we removed all records for non-DOI entities.

Assuming that the bureaus would continue their current cellular plans, we calculated potential savings (present value) over the next 3 years by multiplying the total annual cost by the 3-year discount rate established by the Office of Management and Budget. Because our review included only four bureaus and was limited to one cellular service provider, Verizon Wireless, we believe our savings estimate is conservative.

	Identified Savings (Questioned Costs)	**Potential Savings Over Next 3 years** (Funds to be Put to Better Use)
Unused mobile devices	$605,646	$1,763,423

Appendix 3: Response to Draft Report

The Office of the Chief Information Officer's response follows on page 16.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

MAR 3 0 2016

MEMORANDUM

To: Mary L. Kendall
Deputy Inspector General

From: Sylvia Burns, Chief Information Officer

Subject: Office of the Chief Information Officer Response to Draft Audit Report, *U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices, Report No. 2015-ITA-032*

The Office of the Chief Information Officer (OCIO) for the Department of the Interior appreciates the opportunity to review the Office of the Inspector General (OIG) Draft Audit Report. We have discussed the recommendations with the impacted bureaus (USGS, FWS, NPS, and BLM). Pursuant to your request, the OCIO submits the attached *Statement of Actions* for implementation of the OIG's recommendations as noted in the draft report.

If you have any questions, please contact me at (202) 208-6194. Staff may contact Steven B. Thompson, Acting Director, Compliance and Audit Management (CAM) at (202) 821-8887.

cc: Alexandra Lampros, Financial Specialist, Office of Financial Management
Steven B. Thompson, Acting Director, Compliance and Audit Management
Kristen Sarri, DAS-PMB
Elena Gonzalez, DAS-TIBS, PMB
Olivia Ferriter, DAS-BFPA, PMB
Amy Holley, Chief of Staff, PMB
Debra Sonderman, PAM
Denise Flanagan, POB
Douglas Glenn, PFM
Alexandra Lampros, PFM
Steven B. Thompson, OCIO
Mark Sogge, USGS
Tim Quinn, USGS
Alan Wiser, USGS
Ken Taylor, USFWS
Susan Gabriel-Smith, BLM
Shane Compton, NPS
DOI ADIRs
OCIO ELT

Attachments:

1. OCIO Statement of Actions to Address Office of Inspector General Draft Audit Report U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices, Report No. 2015-ITA-032

Attachment 1

Office of the Chief Information Officer
Statement of Actions to Address Office of Inspector General Draft Audit Report
U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices, Report No. 2015-ITA-032

Background and Observations

The Department of the Interior (DOI) relies heavily on a broad array of mobile and cellular devices and services to fulfill our mission objectives and to support the health and safety of our employees. The DOI Office of the Chief Information Officer (OCIO) supports these activities by coordinating with leadership across the organization to: (1) establish policies, processes and controls to ensure the appropriate stewardship of mission data and government resources; and (2) establish and support mandatory use, DOI-wide contracts and shared services to optimize the appropriate and efficient utilization of mobile devices and services across the enterprise.

The OCIO and named bureaus each received two Notices of Potential Findings and Recommendations (NPFRs) in summer, 2015, related to the OIG Mobile Computing Device Management Audit (OIG 2015-ITA-032). The first concerned "unused" mobile devices. This Finding is provided in the Draft Audit Report.

Inventory of Mobile Devices and Services

As evidenced by our comprehensive cellular wireless initiatve, which includes plans for an enterprise acquisition mechanism and associated policy and procedural changes, DOI agrees that the Department needs to better manage its cellular devices and services.

However, the magnitude of the financial impact estimated in this Draft Audit Report may be materially overstated due to the scope and quality of the data underpinning the Audit. Our specific concerns regarding the data include the following:

- State Wildlife agency lines of service identified as US Fish and Wildlife Service (FWS);
- State district attorneys and the Oklahoma Department of Human Services lines of service identified as US Geological Survey (USGS);
- Confirmed "Terminated" lines of service appeared in the report;
- Confirmed "Suspended" lines of service appeared in the report;
- Verizon disclaimed the information provided, stating that the data "was neither audited nor verified."

The Department further asserts that retaining "unused" and "ready-to-use" mobile devices may be both necessary and prudent to fulfill mission and legal requirements including but not limited to: wildland fire management, law enforcement, support for rotating seasonal workforce, records retention and legal discovery.

Security of Mobile Devices

The second NPFR issued to the OCIO and named bureaus pertained to the security of mobile devices themselves. This Finding and its associated Recommendations, numbers three and four, are also presented in the Draft Audit Report. The OCIO agrees with the spirit of the Recommendations, but respectfully submits that it cannot concur with them as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management (MDM) solution. Nor is it necessary or fiscally responsible to maintain one-to-one parity of device inventory with MDM licensing and enrollment counts. Bureaus and offices routinely have legitimate business reasons for maintaining un-provisioned devices. Similarly, certain mobile devices cannot be managed using the Department's MDM solution, and are managed instead using the Department's standard client management tools, and/or are not data consumption devices. Figures and device totals presented in support of the Finding do not appear to take these conditions into account. DOI has committed to secure mobile devices that process DOI data in accordance with the Guidelines provided in National Institute of Standards and Technology (NIST) Special Publication 800-124 Revision 1, which is footnoted in the Draft Audit Report on page 7.

Response to Recommendations

Recommendation 1: ***Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services.***

Response: OCIO concurs with the recommendation. The GAO made three recommendations in their Report, "Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services, GAO-15-431, May 2015. They are:

1. Ensure the establishment of a Department-wide inventory of mobile devices and services (i.e., all components' devices and associated services are accounted for)
2. Ensure a reliable Department-wide inventory of mobile service contracts is developed and maintained
3. Ensure Procedures to Monitor and Control Spending are established Department-wide. Specifically, ensure that:
   - Procedures include assessing devices for zero, under, and over usage;
   - Personnel with Authority and Responsibility for Performing the Procedures are Identified; and
   - The specific steps to be taken to perform the process are documented.

As DOI has indicated in its response to the GAO, efforts are underway to resolve and implement each of these three audit recommendations. In order to eliminate duplicate effort and unnecessarily duplicative administrative requirements, DOI requests clarification of this Recommendation, recognizing that it should be addressed and reported exclusively by reference to the associated and pre-existing GAO Audit Recommendation.

Responsible Official & Title: Jerry Johnston, Director, Information and Technology Management Division

Lead Contact & Title: Andrew Havely, Chief, Solutions Design and Innovation

Target Completion Date: Resources Permitting: 12/31/2016 (the same as the current target completion dates of all three GAO audit recommendations)

Recommendation 2: ***Implement an enterprise-wide approach for procuring and managing DOI mobile devices.***

Response: OCIO concurs with the recommendation. Efforts are underway to resolve and implement this recommendation through contract action and associated policies and procedures for the utilization of cellular devices and services.

Responsible Official & Title: Jerry Johnston, Director, Information and Technology Management Division

Lead Contact & Title: Andrew Havely, Chief, Solutions Design and Innovation

Target Completion Date: Resources Permitting: 12/31/2016 (the same as the current target completion dates of all three GAO audit recommendations)

Recommendation 3: ***Verify that DOI's mobile device management solution (e.g., MaaS360) manages all mobile devices distributed to employees and contractors.***

Response: OCIO cannot concur with the recommendation as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management (MDM) solution. Similarly, certain "mobile devices" cannot be managed using the Department's MDM solution, and are managed instead using the Department's standard client management tools, and/or are not data consumption devices. Nor is it necessary or financially responsible to maintain one-to-one parity of device inventory with MDM licensing and enrollment counts: Bureaus and offices have legitimate business reasons for keeping certain unprovisioned devices and lines of service active for rapid redistribution or transfer when cancellation and new cellular service activation would otherwise negatively impact the mission.

The Department will secure mobile devices that process DOI data in accordance with the Guidelines provided in NIST SP 800-124 Revision 1. We recommend, and can concur with, this language in the final report.

Responsible Official & Title: Karen Matragrano, Acting Director, Service Delivery Division

Lead Contact & Title: Trent Randall, Unified Messaging Chief, End User Services Branch

Recommendation 4: ***Enroll newly acquired mobile devices into DOI's mobile device management solution within 72 hours of issuing the devices to individual users***

Response: OCIO cannot concur with the recommendation as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management solution. However, the Department will issue a clarifying directive that mobile devices that process DOI data are to be secured in accordance with the Guidelines provided in NIST SP 800-124 Revision 1 within 72 hours of issuance to individual users. We recommend, and can concur with, this language in the final report.

Responsible Official & Title: Lawrence Ruffin, DOI Chief Information Security Officer

Lead Contact & Title: Chris Rutherford, DOI Deputy Chief Information Security Officer

Appendix 4: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer (OCIO) concurred with two recommendations and did not concur with two recommendations (see Appendix 3). OCIO's response also included an action official for each recommendation and target dates for the two recommendations with which it concurred. Based on the response, we consider three recommendations resolved but unimplemented and one recommendation unresolved.

Recommendations	Status	Action Required
1, 2, and 4	Resolved but unimplemented.	We will refer these recommendations to the Office of Policy, Management and Budget to track implementation.
3	Unresolved.	We will refer this recommendation to the Office of Policy, Management and Budget for resolution.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081
Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240