OFFICE OF INSPECTOR GENERAL
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Audit of NARA's Mobile Device Management

OIG Audit Report No. 15-02

November 12, 2014

Table of Contents

Executive Summary

Mobile devices, such as smartphones, personal digital assistants (PDAs), and tablet computers have become increasingly popular with today's highly mobile workforce. They allow employees to perform tasks at any time and from any place, as well as transport large volumes of data efficiently. The National Archives and Records Administration (NARA) provides mobile devices to eligible employees to improve communication and productivity. However, there are security threats that need to be mitigated in order to support confidentiality, integrity, and availability of the data and applications on the devices.

NARA's Office of Inspector General (OIG) performed an audit of NARA's Mobile Device Management. The overall objective of this audit was to evaluate NARA's efforts to secure and deploy mobile devices on the NARA network, and to maintain and dispose of these devices. Specifically, we determined whether: (1) adequate policies and procedures have been implemented; (2) NARA maintains an accurate inventory of its mobile devices; (3) effective controls are in place to protect the information stored or processed on the mobile devices; and (4) NARA is prepared to handle supply chain threats and expand its mobile device portfolio.

In general, it appears NARA's mobile devices are effectively managed, utilizing a centralized management server system and the technical expertise of NARA employees and contractors. However, deficiencies were noted in managing device use and phone lines, ensuring logical security of the device and data, and developing a strategic plan for mobile device portfolio expansion.

Users who violated NARA's mobile device use policy were not held accountable, and no policies and procedures exist to determine when a reimbursement or disciplinary action will be required for inappropriate or excessive use. For fiscal year 2013, charges related to inappropriate or excessive use were estimated to be $2,745. In addition, NARA did not always ensure only one phone line was activated for a user, resulting in spending approximately $7,289 for duplicate phone lines until they were disconnected in response to our audit. Combining the two, NARA incurred unnecessary spending of approximately $10,034 which could have been put to better use.

Further, logical security controls, including controls for interaction with other systems, user authentication, and lockout settings, were either not implemented or inconsistent with NARA policy. Also, NARA did not always ensure data on lost or retired mobile devices was completely sanitized, and the inventory of retired mobile devices was

outdated and inaccurate. The lack of controls to properly secure devices and data increases the risk of unauthorized access to devices and sensitive personal or agency data.

Finally, NARA provides only one type of smartphone, BlackBerry devices, to employees. No strategic plan to expand NARA's mobile device portfolio has been developed. This may jeopardize the mobile computing and communication capability at NARA in the event these devices become obsolete, become vulnerable, or if something should happen to the supply of these devices in the market.

Most of these deficiencies exist because strong internal controls including detailed and clearly defined policies and procedures were not implemented; and effective performance monitoring and oversight had not been conducted for managing NARA's mobile devices. This report contains 10 recommendations which, upon implementation, will assist NARA in effectively managing its mobile devices and data on them.

Background

NARA has provided mobile devices to approved employees since 2002. As of December 2013, NARA had a total of 438 participating lines including BlackBerry smartphones, cellular phones, and wireless modems. The majority of mobile devices issued by NARA to its employees are BlackBerry smartphones. Blackberry smartphones represent over 80% of the mobile communication devices deployed at NARA. For the period October 2012 through September 2013, NARA spent an average of $24,007 monthly or $288,079 annually for mobile service.

NARA's Office of Information Services (I) is responsible for performing various tasks related to managing NARA-issued mobile devices and their data security. It orders devices for approved NARA employees, activates and deactivates them, and works with the BlackBerry Enterprise Server (BES) management contractor to manage NARA's BlackBerry configurations. The contractor started managing the BES environment for NARA in April 2013. Prior to that, this environment was managed under NARA's main information technology contract, NARA Information Technology and Telecommunication Support Services (NITTSS). Currently, NITTSS assists NARA's Office of Information Services in performing activation, local wipe, and incident handling for NARA's mobile devices.

Currently, NARA's BES servers are located in a data center in Phoenix, Arizona, where their security and availability is maintained by a colocation service provider. We reviewed the independent auditor's Service Organization Control reports relevant to security and availability (SOC 1 and SOC 2) covering the period of July 1, 2013, through December 31, 2013, for the service provider. Per review of the reports, we noted adequate controls were in place at the contractor's facility to support physical and logical security, as well as availability of the systems hosted in the facility.

NARA has been a customer of BlackBerry devices since 2009. Currently, the BlackBerry devices are the only type of smartphones NARA provides to employees. There were two pilot projects in fiscal year 2011 intended to evaluate the usefulness of DROID phones and iPads in NARA's work environment. Many of the participants stated they provided certain benefits including easy access to the Internet, taking and sharing notes, and visual presentation capabilities. The participants stated job efficiency would increase by utilizing those features at NARA.

In addition, the two pilot projects revealed the need to (1) improve the cellular signal coverage at Archives I and II; and (2) develop mobile interfaces of NARA's web site. To improve cellular signal coverage, NARA contracted with an IT services company in September 2013 to install a Distributed Antenna System (DAS) at Archives II. This effort has a planned completion date of September 2014. Upon completion, it is expected the cellular voice and data coverage inside the Archives II facility will be improved for the nation's major wireless service providers (WSPs). In addition, NARA's Office of Innovation (V) intends to create mobile interfaces for both Archives.gov (NARA's public-facing web site) and nara-at-work.gov (NARA's intranet). However, no specific work has begun to accomplish these goals.

Objectives, Scope, Methodology

The overall objective of this audit was to evaluate NARA's efforts to secure and deploy mobile devices on the NARA network, and to maintain and dispose of these devices. The specific objectives of this audit were to determine whether: (1) adequate policies and procedures have been implemented; (2) NARA maintains an accurate inventory of its mobile devices; (3) effective controls are in place to protect the information stored or processed on the mobile devices; and (4) NARA is prepared to handle supply chain threats and expand its mobile device portfolio.

Based on National Institute of Standards and Technology (NIST)'s scope on its Special Publication (SP) 800-124 Revision 1, "*Guidelines for Managing the Security of Mobile Devices in the Enterprise*", dated June 2013, we focused on the security controls around NARA-issued BlackBerry smartphones. At NARA, BlackBerry smartphones comprise over 80% of the organization-issued mobile device portfolio, and they have data storage/exchange capabilities. Devices with minimal or no computing capability, such as basic cellular phones and wireless modems, were excluded from this audit. Also, although NARA has acquired about 37 tablet computers since 2011, they were excluded from this audit because they do not connect to NARANet[1] or use a mobile e-mail exchange solution like the BlackBerry smartphones. Further, we excluded laptops from this audit due to the different security controls available for them.

To accomplish our audit objective, we reviewed documents describing NARA's policies and procedures for managing mobile devices. We also reviewed applicable requirements and guidelines, including NIST SP 800-124 Revision 1 "*Guidelines for Managing the Security of Mobile Devices in the Enterprise*", dated June 2013; NIST SP 800-53 Revision 4 "*Security and Privacy Controls for Federal Information Systems and Organizations*", dated April 2013; Department of Defense (DoD)'s "*Wireless Security Technical Implementation Guides (STIG)*", Version 5, Release 2.2, dated September 15, 2008; and Federal Chief Information Officer (CIO) Council and Department of Homeland Security (DHS)'s "*Mobile Security Reference Architecture*", dated May 23, 2013. We conducted interviews with key personnel in the Office of Information Services (I) and Office of Innovation (V) to determine whether the mobile device management at NARA is in accordance with documented internal policies and procedures, as well as Government-wide requirements and guidelines.

[1] NARA's unclassified computer network that provides access to NARA intranet, e-mail, and the Internet

In addition, in order to determine whether retired mobile devices and any data on them are appropriately managed, we tested a judgmental sample of 20 retired mobile devices. The results of a non-statistical sample cannot be projected to the intended population. We also reviewed the monthly wireless service bills for the period of October 2012 through September 2013 to determine if users complied with NARA's mobile device use policy.

Our audit work was performed at Archives II in College Park, MD, between September 2013 and July 2014. We conducted this performance 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

1. Mobile Device Use Policy Needs to be Enforced

We found the policies and procedures for using NARA-issued mobile devices were not consistently followed. There were users who incurred additional charges due to inappropriate or excessive use of the device. We also found some users were issued more than one mobile phone device. This occurred because (1) a strong internal control process had not been established to identify noncompliance and reduce cost; and (2) sufficient training had not been provided to the users of NARA's mobile devices to reinforce the policies and procedures. NARA issued Interim Guidance 813-1 (NARA 813-1), "*NARA-issued BlackBerry Personal Digital Assistants (PDAs)*[2]", on March 9, 2011, to provide updated requirements and procedures for employees issued BlackBerry devices. In addition, NARA Directive 802 (NARA 802), "*Appropriate Use of NARA Office and Information Technology (IT) Equipment and Resources*", issued May 21, 2012, included definitions of appropriate and inappropriate use of NARA-owned wireless communication devices. The failure to properly follow the policies and procedures resulted in not only additional money spent on the wireless service bills but also potential compromise of data stored on the mobile devices. Our audit results are discussed in more detail below.

Users did not obtain a travel BlackBerry for international travel

Mobile devices are susceptible to theft, hackers, and abnormal wear and tear during foreign travel. In addition, certain countries reserve the right to confiscate electronic devices containing encrypted data. Therefore, NARA 813-1 states individuals with a need for BlackBerry service outside the United States and Canada for official NARA travel must obtain a travel BlackBerry device. Obtaining a travel device limits potential exposure of e-mail and e-mail attachments exchanged during the trip.

As of September 2013, NARA had two travel BlackBerry devices with plans covering unlimited global e-mail and data. NARA maintains the travel BlackBerry devices for users who need BlackBerry service during international travel. During our test period of October 2012 through September 2013, NARA spent $1,625 to maintain the wireless service plans for these travel devices. However, these devices were not always efficiently

[2] A PDA traditionally refers to a mobile device used for accessing the Internet, exchanging e-mail, and organizing data without phone services. A smartphone has both phone services and PDA features like the BlackBerry devices NARA currently uses. Therefore, the terms "BlackBerry smartphone" and "BlackBerry device" are used in this report instead of "BlackBerry PDA".

utilized. Specifically, we found there were NARA employees who took their non-travel, NARA-issued BlackBerry devices to foreign countries, which is a violation of NARA policy.

We reviewed the monthly wireless service bills for the test period and found there were at least 14 users who incurred global roaming charges, in addition to their monthly plan charges, by taking their non-travel BlackBerry devices to foreign countries. These countries included Canada[3], Mexico, the United Kingdom, Poland, France, Switzerland, Haiti, Germany, Belgium, and Ireland. One user incurred the charge for three consecutive months, which, for that user alone, totaled $304. The total global roaming charges for the 14 users, was $1,266. Further, we found there were six months during the period where one or more of the travel devices were available for the entire month. Although four of the six months overlapped with the months the 14 users traveled overseas, they did not obtain a travel device[4]. **Table 1** summarizes the global roaming charges incurred by taking non-travel devices on international travel.

In order to understand the reason the violations occurred, we made inquiries with two representatives from the Office of Information Services (I) regarding NARA's BlackBerry user training process and whether the travel policy is covered within the training. One employee stated although a short review of the device is given to the user upon receipt of the device, international travel is not covered during the review because there are only a handful of users who request international travel each year. An IT Security Specialist stated the annual Security Awareness training includes information also applicable to mobile devices, yet no information regarding the requirement to obtain a travel device was included in the training.

According to one employee, she has been reviewing the monthly wireless bills and contacting the users for excessive or inappropriate use. However, she was not able to provide documented evidence of monthly reviews prior to June 2013. Further, although there were users who incurred global roaming charges after June 2013, we were unable to obtain evidence that the employee contacted the users regarding the charges. According to the employee, most times the discussions took place verbally via telephone and were not documented.

[3] Although NARA 813-1 requires obtaining a travel device for a travel outside the United States and Canada, we found international roaming charges were also applied to travels to Canada. According to an Office of Information Services representative, NARA is currently in the process of updating the agency's mobile device policy to reflect the information more accurately.

[4] During a meeting subsequent to the issuance of the draft audit report, management stated the employees who took their BlackBerry devices overseas might have been approved to do so due to the unavailability of travel BlackBerry devices. However, NARA 813-1 does not allow for taking non-travel BlackBerry devices overseas when there are no travel devices available.

Table 1: Summary of Global Roaming Charges[5]

User	Months Traveled	Were Travel Device(s) Available?	Location	Roaming Charge
User 1	November 2012 thru January 2013	Yes	Belgium, Haiti, Ireland, UK	$304
User 2	March 2013	Yes	International Cruise	$194
User 3	October 2012	No	Canada	$125
User 4	July 2013	No	Germany, Ireland	$116
User 5	October & November 2012	Yes	Poland, UK	$96
User 6	November & December 2012	Yes	Germany	$94
User 7	June 2013	No	Canada	$73
User 8	October 2012	No	France, Switzerland	$68
User 9	July 2013	No	Canada	$59
User 10	May 2013	No	Canada	$41
User 11	October 2012	No	Canada, UK	$37
User 12	January 2013	No	International Cruise	$36
User 13	October 2012	No	Mexico	$16
User 14	August 2013	Yes	International Cruise	$8
			Total	**$1,266**

Mobile devices add security risks due to the susceptibility to data exfiltration and eavesdropping when they transmit data through telecommunication networks. Such risks are even more heightened when users are on international travel in countries where the networks are controlled by the host government. In such case, traveling in these countries makes it easier for the government to monitor any transmissions executed on mobile devices. Therefore, depending on the quantity and content of the data stored on a non-travel NARA-issued BlackBerry, taking it to foreign countries could result in disclosure and misuse of sensitive personal, agency, or government data in case the device became compromised.

[5] This summary was based on global roaming charges of $7.50 or more per user per month. However, during a meeting subsequent to the issuance of the draft report, management indicated $7.50 was not a correct threshold for global roaming charges because NARA 601, NARA Travel Policy, is the governing policy for calls made by NARA employees during travel. However, the employee responsible for performing the review had not made a distinction between global roaming charges and other additional charges and consistently used $7.50 as a threshold for all additional charges in her review. Further, NARA 601 is a policy for the Government to reimburse the employees, not for the employees to reimburse the Government, and it does not include a monetary threshold for international calls. Therefore, for consistency, we used the threshold of $7.50 for conducting our independent analysis of the charges.

Users were not held accountable for excessive use of device

According to NARA Directive 802, NARA staff is authorized to use NARA's IT equipment (including wireless communication devices) when conducting official NARA business and performing limited personal use during non-work time (such as making limited personal phone calls and sending and receiving limited personal e-mail messages). However, if any personal use of NARA equipment generates more than minimal additional expense to NARA, it is considered inappropriate use. The Directive also states, although users may make personal calls with their NARA-issued cellular telephone or PDA, the user will be liable for the cost of personal calls that result in charges exceeding the basic contract rate that NARA pays for cellular service[6].

We reviewed the monthly wireless service bills to identify any charges of $7.50 or more in addition to the user's monthly contracted plan charge that might be non-business-related. The threshold of $7.50 was used in our analysis to be consistent with the employee mentioned above's approach of reviewing the bills.[7] Our review found most users appeared to have only minimal (less than $ 7.50 per month) or no additional charges due to personal use. The number of users who had additional charges of $7.50 or more ranged from two to 15 per month. The two main categories where the additional charges occurred were global roaming and messaging **Table 2** summarizes the service categories and cost for each category where those additional charges occurred.

Table 2: Summary of Additional Charges

Category	No. of Users	Cost
Global Roaming	14	$1,266
Messaging	16	$1,101
National Roaming	5	$202
International Long Distance	3	$76
Application Download	1	$53
411 Search	5	$46
Total	**37**[8]	**$2,745**

[6] Appendix A of NARA Directive 802 describes examples of calls necessary in the interest of the Government and includes emergency calls and some types of personal calls in the "official business calls" category. Therefore, users will not be held liable for the calls made in this category.

[7] The employee and IT Service Chief agreed to use $7.50 as the threshold for reviewing the bills on a monthly basis in June 2013. According to the employee, it changed to $10.00 in January 2014, after having a discussion with the CIO.

[8] This is not a sum of the users in each category because there were users who had additional charges from more than one category.

- International Roaming - As previously stated, the total cost due to global roaming on non-travel BlackBerry devices was $1,266.
- Messaging - Although individuals may use messaging to some extent for conducting official NARA business, we found there were users who showed a pattern of significantly exceeding their monthly contracted plan charges. For example, one user exceeded the plan by $46 to $84 per month for six months due to text messaging. In addition, there were seven users who subscribed to one or more premium messaging[9] programs for up to seven months. These premium messaging programs usually cost $9.99 per phone number per program. Although the bills did not include details on the contents provided by the programs, some of their titles clearly indicated they were for personal entertainment (e.g., "My IQ Quiz"). The total cost of these messaging services for the period was $1,101.

The reasons the additional charges occurred or were not reduced were the following:

1) Unclear Instructions – Consistent with NARA 802, it is reinforced during the annual Security Awareness training that misuse or inappropriate use of NARA assets include personal use that could generate more than minimal additional expense to NARA. However, for the use of NARA-issued mobile devices, guidelines have not been provided to the users as to what would be considered "minimal additional expense".
2) Unrequested Reimbursements – According to the Chief of the IT Service Branch, NARA has not sent out any letters for reimbursements because NARA 813-1 does not require reimbursement.
3) Inadequate Review of Service Plans – According to the responsible NARA employee, when additional charges of $7.50 or more are detected on the monthly bills, she contacts the user to identify the reason and discuss switching plans to better accommodate the user's needs while saving the overall cost. However, we found the switch did not always occur in a timely manner; in one case, a new service plan was not applied to the user's number until the user had additional charges ranging from $46 to $84 per month due to text messaging for at least six consecutive months, as stated previously.
4) Application download – NARA's BlackBerry Enterprise Server (BES), a server centrally managing BlackBerry configurations, blocks the BlackBerry users from downloading applications. However, there is no physical or logical mechanism that prevents the traditional cellular phone users from downloading applications. According to the responsible NARA employee, the only way she could stop the

[9] Messaging programs provided by third party content providers at additional charge

charges related to downloaded applications is to review the monthly statements and contact the user to uninstall the application, which was not always completed.

As a result, we found there were 37 individuals who had additional charges of $7.50 or more, totaling $2,745 for the testing period, which could have been put to better use.

NARA was paying for more than one phone line per user

During our review of the wireless service bill for September 2013, we found there were users with more than one phone number. Per inquiries with the responsible NARA employee, we found there were 14 phone numbers in which incorrect names of the users were assigned, which made the users appear to have multiple phone lines. Further, there were four users who had more than one active phone line incurring monthly charges. For example, there was a phone number activated in March 2003 which had been costing $28 - $30 per month until it was disconnected in November 2013 in response to our audit inquiry. The total estimated cost of keeping the phone line from March 2003 through November 2013 was $3,692. According to the bill, the number was under the name of the IT Service Branch Chief. However, she stated she never used the number, she did not know who the previous user was, or why it was under her name.

Another example was associated with an employee who already had a NARA-issued cellular phone and requested a BlackBerry device. Although a BlackBerry device was issued to him, the cellular phone he was already using was never returned or asked to be returned. According to the Telecommunication Specialist, the employee stated he was using the BlackBerry for e-mail and cellular phone for phone calls. When we calculated the cost of having duplicate phones since the time his BlackBerry was activated in January 2010, it was estimated to be $48 - $50 per month with a total cost of $2,202.

NARA was paying for more than one phone line per user because NARA failed to (1) disconnect phone lines in a timely manner when they were no longer needed; and (2) verify whether the user had an existing phone line before a new line was activated. When we brought this to the relevant employee's attention, she admitted both instances occurred due to an oversight. As shown on **Table 3**, the total estimated cost of maintaining duplicate phone lines for all of the four users was $7,289[10], which could have been put to better use.

[10] Only estimates were available for the costs for September 2012 and earlier, because the oldest monthly statement the Telecommunication Specialist was able to provide was October 2012. According to the Telecommunication Specialist, the monthly rates had not changed in recent years.

Table 3: Cost of Duplicate Phone Lines

Phone Line	Active Since	Monthly Cost[10]	Total Cost[10]
Line 1	March 2003	$28 - $30	$3,692
Line 2	May 2010	$28 - $45	$1,221
Line 3	January 2010	$48 - $50	$2,202
Line 4	August 2013	$49 - $52	$175
		Total	**$7,289**

Recommendations

We recommend NARA’s Chief Information Officer:

1. Develop and document a strong internal control process for:
    a. Ordering, activating, and deactivating mobile devices and phone lines to ensure no unnecessary phone lines exist and incur cost;
    b. Reviewing monthly bills for items including user names, activities, plan adequacy, and opportunity for cost saving; and
    c. Determining when an additional charge will be considered for reimbursement.
2. Review and update NARA’s current policy documents for use of NARA-issued mobile devices, including NARA 813-1 and NARA 802, to reflect more complete and accurate information on acceptable uses of the devices and when a disciplinary action will be required.
3. Provide training to educate users on acceptable uses of NARA-issued mobile devices, including requesting a travel device for international travel.

Management Response

Management concurred with the recommendations.

2. Logical Security on Active Devices Needs to be Enhanced

We found the security settings on NARA’s BlackBerry devices were generally in compliance with NARA policies and recommendations found in external sources such as NIST publications and DoD’s Wireless STIG. However, deficiencies were identified in device interaction with other systems, password requirements, and lockout settings. These deficiencies existed because policies and procedures have not been fully developed, and the existing policies were not properly implemented. NIST SP 800-124 states organizations should fully secure each organization-issued mobile device before allowing a user to access it, and then should regularly maintain mobile device security to protect the device from threats. Failure to strengthen security controls may lead to (a) unauthorized use of the device and data; (b) infecting the device and any other device it interacts with; and (c) a failure to detect data compromise and other malicious activity on the device. Our audit results for each of these areas are discussed in more detail below.

No adequate guidance exists for interaction with other systems

According to NIST SP 800-124, when mobile devices interact with other systems in terms of data exchange and storage, the organization's data is at risk of being stored in an unsecured location outside the organization's control, and there is also a possibility of malware transmission from device to device. Therefore, preventing an organization-issued mobile device from syncing with a personally-owned computer necessitates security controls on the mobile device to restrict what devices it can synchronize with.

Both NARA Directive 1608, "*Protection of Personally Identifiable Information (PII)*", issued on August 6, 2009, and the Telework Agreement (NA Form 3040) disallow downloading or storing data containing PII on a personal computer where other individuals may have access to it. However, NARA 813-1, the main policy document for NARA-issued BlackBerry users, does not provide any guidance on interaction of NARA-issued BlackBerry devices with other systems, including personally-owned or public computers. A NARA IT Security Specialist agreed this should be an element of the formal mobile device use policy. Further, NARA currently does not have a technical control to limit the interaction to exchanging only PII- and malware-free files and data. A failure to (1) fully develop and inform the users of the device interaction policy; and (2) implement a technical control to support the policy may lead to disclosure of sensitive information (including organization data and PII) and malicious files being transferred and spread across NARA's network.

User authentication on BlackBerry needs improvement

NARA's Enterprise Architecture requires for all data, the information system to enforce minimum password complexity of a case-sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each. It also requires the information system enforce at least a four-character change when new passwords are created, restrict password minimum and maximum life time to be between one and 90 days, and prohibit reusing the previous five passwords for unclassified information systems. Our review of the password requirements on NARA-issued BlackBerry devices revealed they do not fully comply with the requirements in the Enterprise Architecture. **Table 4** compares the requirements

In addition, the Homeland Security Presidential Directive-12 (HSPD-12) calls for a mandate, government-wide standard for secure and reliable forms of identification (ID) issued by the Federal Government for access to federally-controlled facilities and networks. The Directive states the heads of the agencies shall, to the maximum extent practicable, require the use of ID by Federal employees and contractors that meets the standard, a Personal Identity Verification (PIV) card, for example, in gaining physical access to federally controlled facilities and logical access to federally controlled information systems. Further, NIST 800-124 recommends more robust forms of authentication than just a password, such as multi-factor authentication using a security token, be implemented before gaining access to the mobile device or the organization's data accessible through the device. However, we found NARA does not require a PIV card or other types of multi-factor authentication to log onto the agency-issued mobile devices[11].

NARA implemented the SecureAuth multi-factor authentication to access Google Apps (including e-mail) from non-NARA devices. However, for NARA-issued BlackBerry devices, once the user logs on to the device by inputting the device password, there is no other user authentication required to access NARA e-mail. Further, the password requirements on BlackBerry devices are not as stringent as required in the Enterprise Architecture. For example, our test revealed passwords containing only letters such as "QWERTYUI" and "ASDFASDF", made up of the keys sequentially located on BlackBerry's keypad, were allowed.

According to NARA's BES management contractor, when a user is issued a BlackBerry device, the user inputs a one-time activation code during the activation process to enable the synchronization between the server and the device for email, organizer data, and any previous backup files. The activation code is created and provided by the BES management contractor, and once the activation is completed, no additional user setup is required to access email or calendar than the device password.

As mobile devices are more susceptible to misplacement and theft, it is critical to maintain a strong authentication mechanism in order to protect the data on them. By relying on a less stringent authentication mechanism, NARA's mobile devices and the

[11] During a meeting subsequent to the issuance of the draft audit report, management stated NARA's BlackBerry devices have two-factor authentication because they satisfy the requirements of (1) something the user has (the device) and (2) something the user knows (password). However, we determined the possession of a BlackBerry device does not satisfy the requirement of "something the user has" because (a) the user's identity is verified via a PIV card only at the time the device is picked up; and (b) when the device is fallen unto un-trusted hands, only one attribute, the password, is required to access the device and all data accessible through the device.

data on them are at risk of unauthorized access and a loss of confidentiality, integrity, and availability of the data and applications on them.

Table 4: Password Requirements

Requirement	Enterprise Architecture	BlackBerry Configuration	Compliant?
Minimum Password Length	8	8	**Yes**
Maximum Password Age	90	90	**Yes**
Password Pattern	Case-sensitive Mix of Upper Case Letters, Lower Case Letters, Numbers, and Special Characters, Including at least One of Each	No Restriction Except Identical Characters, (e.g., 11111111) Sequences (e.g., 12345678), "NARA", or "Password"	**No**
Maximum Password History	5	3	**No**
Character Change	At Least 4 Character Change when New Password is Created	-	**No**

BlackBerry devices are not locked when holstered

According to NIST SP 800-124, one of the security services organizations may consider implementing in combination with other types of security services is automatically locking idle devices and remotely locking devices suspected of being left unlocked in an unsecured location. In addition, according to the BlackBerry Policy Reference Guide, locking the device when the user inserts it in a holster is one method to prevent unauthorized use.

Under the security settings for NARA's BlackBerry devices, they are configured to lock after 15 minutes of inactivity, requiring the user to reenter the password. We found this control was in accordance with the Wireless STIG. However, NARA's BlackBerry devices are not configured to lock when the user inserts it in a holster, which is not in accordance with the Wireless STIG and may lead to unauthorized logical access to the device. The risk is even more heightened if the user is traveling via public transportation with his/her BlackBerry holstered in a place easily accessible to other passengers. This may allow an unauthorized user to retrieve any data on the device if they find it within 15 minutes of the authorized user's last use, unless it was manually locked.

Recommendations

We recommend NARA's Chief Information Officer:

4. Develop a formal policy for interaction of NARA-issued mobile devices with other systems and update NARA 813-1 to clearly reflect the policy.
5. Strengthen user authentication for BlackBerry devices by doing one or more of the following:
    a. Strengthening the password requirements for NARA-issued mobile devices to, at a minimum, match the requirements in the Enterprise Architecture; and
    b. Implementing multi-factor authentication to access NARA e-mail and calendar.
6. Re-evaluate the current lockout settings to better protect the data from unintended disclosure and/or misuse.

Management Response

Management concurred with the recommendations.

3. Data Security on Lost Devices Is Not Ensured

NARA lacks an effective lost mobile device management process. We found (1) there is not a centralized list to track lost devices; (2) NARA's incident management system is not consistently used to manage the process; and (3) lost devices are not always reported to the BES management contractor so a remote wipe can be performed.[12] This occurred because the lost device management process was not documented, and management did not provide adequate oversight on performing the steps necessary to safeguard data. NIST SP 800-124 states mobile devices are typically used in a variety of locations outside the organization's control, and their mobile nature makes them much more likely to be lost or stolen than other devices, leading to increased risk of data comprise. Therefore, NIST policy recommends the device be remotely wiped (to scrub its stored data) if it is suspected the device has been lost, stolen, or otherwise fallen into un-trusted hands. The lack of an effective lost mobile device management process may allow missed data sanitization on the device, leading to potential disclosure of sensitive personal or agency information.

We requested a list of the lost or stolen devices reported during fiscal year (FY) 2013 from the responsible NARA employee. However, she stated there is no such list; instead, she provided a set of e-mail communications she had with the users and WSP regarding lost or stolen devices. Since there was no centralized list, we were unable to determine whether the set of e-mail communications represented the entire population of lost or

[12] Remote wipe is a process to remotely erase the data on the mobile device, executed from another machine over a network.

stolen devices for FY 2013. According to the employee, when a user reports a device lost or stolen, she contacts the WSP to suspend the service for the number. However, she was not sure if a remote wipe is performed on the devices and if not, what would happen to the data already residing on them.

Further, the employee stated she remembered only one device reported stolen and not found during FY 2013. However, our review of the e-mail communications revealed there were at least five instances where NARA-issued mobile devices were lost or stolen during FY 2013 and not found. As the responsibility for managing NARA’s BlackBerry Enterprise Server transferred from NITTSS to another contractor during FY 2013, we made inquiries with representatives from both contractors to determine whether any remote wipe command was sent to those devices. The NITTSS representative stated, according to NARA’s incident management system (Remedy), the last lost or stolen mobile device was reported in May 2012. The contractor believed there were no remote wipes done in FY 2013. The representative of the current BES management contractor stated no remote wipes were performed in FY 2013, because no requests were received from NARA.

NARA-issued BlackBerry devices are password-protected and configured to perform an automatic wipe when 10 consecutive incorrect passwords are entered. However, as previously stated, the password requirements on BlackBerry devices are significantly weaker than NARA policy, increasing the risk of password compromise. The weak password requirements and poor management process for lost/stolen mobile devices heighten the risk of data on those devices being accessed by unauthorized users.

Recommendation

We recommend NARA’s Chief Information Officer:

7. Develop a comprehensive lost/stolen mobile device control process to include the following:
    a. All lost or stolen mobile devices are managed on a centralized list with detailed information such as user’s name, phone number, date lost/stolen, date found (if applicable), and status (whether it was wiped, deleted from the server, and disconnected from the wireless service).
    b. The Remedy incident management system is consistently utilized, and any task requiring contractor effort is appropriately communicated to ensure the data on all lost or stolen devices is safeguarded from unauthorized access.

Management Response

Management concurred with the recommendation.

4. Retired Devices Need to be Managed More Effectively

Improvements need to be made in maintaining a complete and accurate inventory and in the process to wipe data from NARA's retired mobile devices. Specifically, (1) the inventory was outdated and inaccurate, and provided no traceability to the previous user or date the device was returned; (2) the retired mobile devices were dispersed throughout the Archives II facility without a coherent storage or recycling plan; and (3) five of the 20 sampled devices were either not wiped or contained pictures on their media cards. These conditions existed because the retired device management process lacked (a) clearly documented policies and procedures; and (b) adequate monitoring and oversight throughout the process. NIST SP 800-124 recommends mobile devices be wiped before being retired to prevent an un-trusted party from recovering any data stored. Mismanaged retired mobile devices may allow personal or agency data to remain on the device, leading to inappropriate disclosure and unauthorized use of the data.

Accurate and complete inventory does not exist

On January 8, 2014, we were provided the most recent inventory of the retired NARA-issued mobile devices, including basic cellular phones, BlackBerry devices, and PDAs NARA used in the past. The inventory contained information such as the models, serial numbers, brands, and vendors. Initially, we planned to take a sample of the retired devices returned during FY 2013 to verify (1) all data were completely wiped; and (2) they were disconnected from the service and properly stored in designated locations. However, the inventory did not include information such as the dates the devices were returned, who previous users were, phone numbers associated with the devices, or where they were stored.

On January 16, 2014, we visited a NITTSS representative in Archives II to obtain a sample of 20 retired mobile devices. During the visit, we observed a total of 34 retired BlackBerry devices composed of the two most recent models (BB9650 and BB9930) NARA provided to employees. However, none of these were included in the inventory.

Further, during the visit, the NITTSS representative stated there should be more retired mobile devices in one of the locked cabinets located in the cubicle of his previous coworker. However, he stated the previous coworker destroyed the key before he left. On January 17, 2014, the NITTSS representative stated he found a total of 189 additional devices from one of the file cabinets within Room 4320, including 170 BB9650 BlackBerry devices. These were also not included in the inventory. According to the NITTSS representative and the responsible NARA employee, the reason why retired mobile devices are dispersed across the Archives II facility is because there is not a single, designated location where they should be stored.

Maintaining an accurate and complete inventory of retired mobile devices provides traceability in the event any residual data requiring the user's attention were found. Due to a lack of an effective inventory management process, NARA's current inventory system for its retired devices does not provide (a) traceability to the previous user; (b) information on whether the devices were properly treated (disconnected and wiped) and (c) the ability to easily identify and physically locate them when necessary.

Data wipe was not always completed

In order to determine whether retired devices are disconnected from the wireless service and there is no residual data on retired devices, we turned on the 20 sampled devices obtained from the NITTSS representative and noted they were no longer receiving signals from the WSP. Also, we were able to obtain estimated[13] dates of the device wipe on some of the devices through the WSP's "Welcome" message, which was automatically sent to the device upon wipe. The dates varied between March 2, 2012 and January 16, 2014; however, because the return dates were unknown, we were unable to determine how timely the wipe was performed.

Among the 20 devices, we found one was not wiped and still password-protected. We noted a total of 55 unread messages (look in the red circle on **Exhibit 1** below) on the device. Because the device was password-protected, we were unable determine what types of data was stored on the device. We intentionally entered 10 incorrect passwords to perform a wipe on the device to remove the previous password in order to verify if there was any content on the media card.[14] We found no content on the card.

Among the 19 wiped BlackBerry devices in the sample, we found four had un-wiped photographs stored on their media cards. According to the NITTSS representative, although he recommends users remove any content on the media card before returning the device, he and his team do not erase them. Per inspection of the photographs stored on the media cards, we noted many of them were taken from NARA meetings and events.

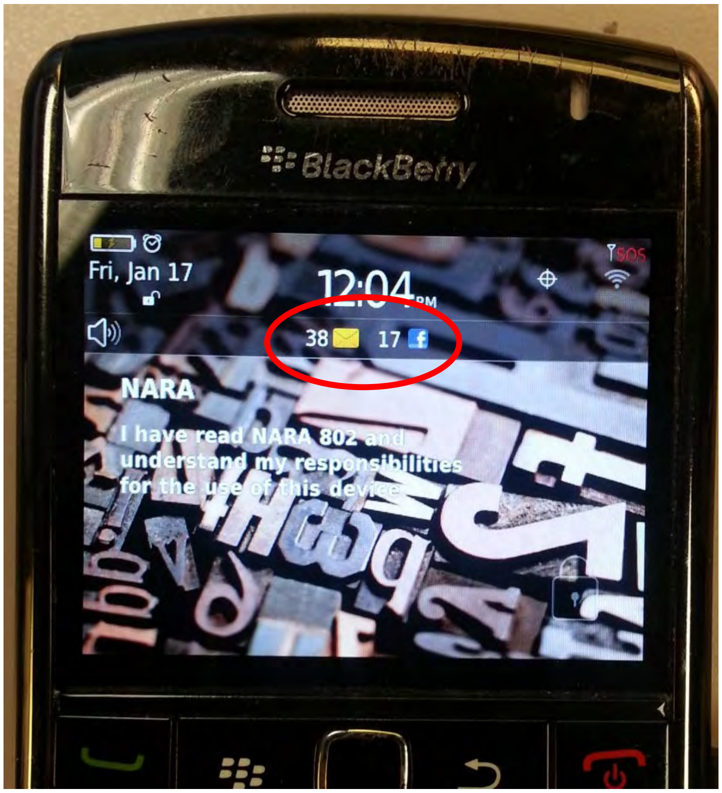
[13] These are estimates as the date of the "Welcome" message from the WSP alone does not provide a definite date of the original wipe performed, because the dates were not confirmed by Remedy tickets or any other tracking mechanism.

[14] A device wipe by itself does not remove any content stored on a media card inserted into the mobile device.

The photographs included images of a NARA event, flowcharts, and discussion topics written on a flipchart (see **Exhibit 2** for the images). In addition to these NARA-related images, we also found personal images, such as portraits, a boarding pass, and vacation photos.

According to the responsible NARA employee, representatives from the Office of Information Services recently had a meeting with a vendor to discuss a recycling program for NARA's retired mobile devices. According to the vendor, it sanitizes all data on the devices before recycling them. However, it is important to ensure NARA takes ownership of the data and safeguards them before the device leaves a NARA facility.[15] A failure to do so may allow an unauthorized person to gain access to and misuse sensitive personal or agency information.

Exhibit 1: A Retired BlackBerry Showing Un-wiped Messages

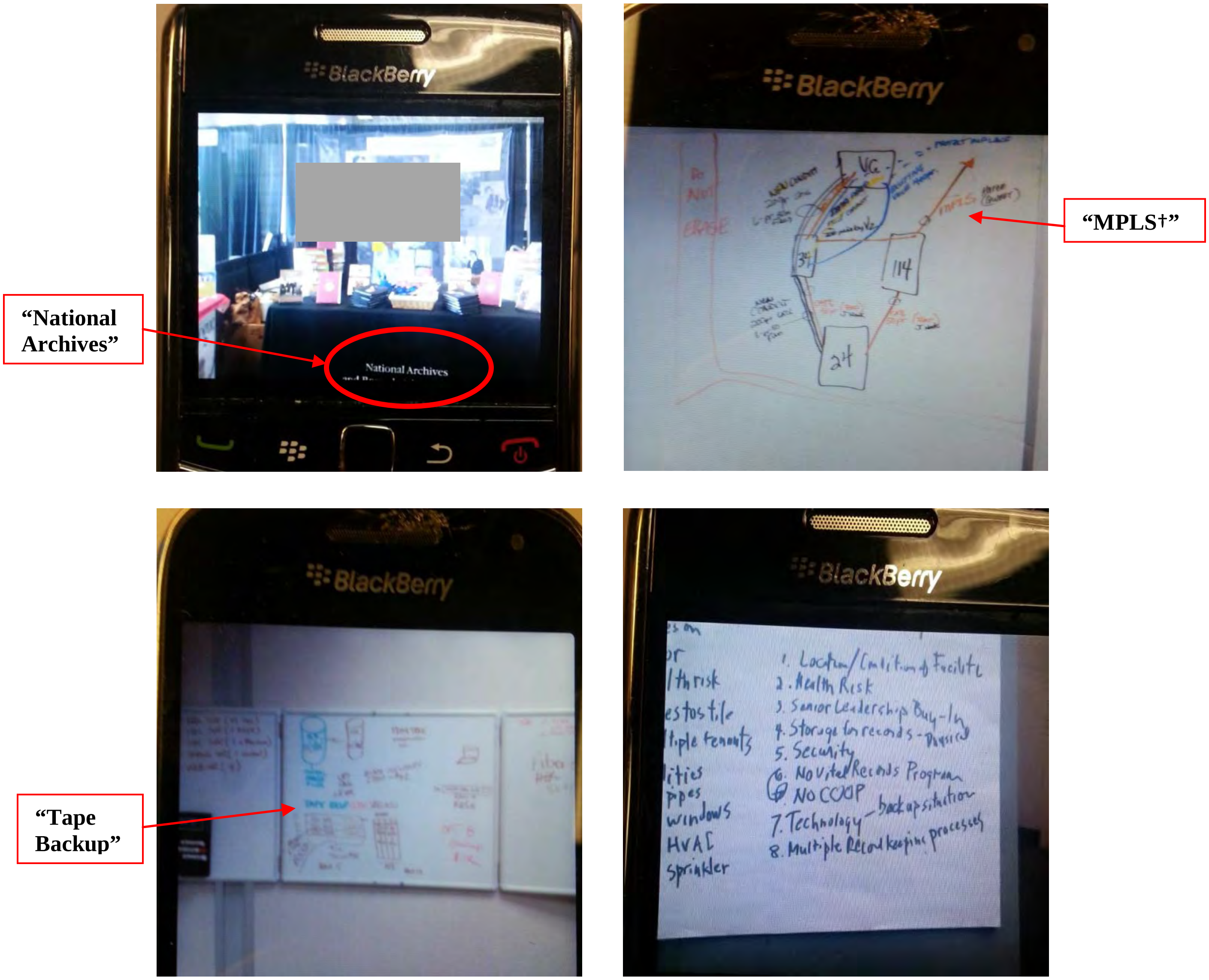


NARA

I have read NARA 802 and understand my responsibilities for the use of this device

[15] According to the Telecommunication Specialist, details for the recycling program are still yet to be determined, and no shipment has been made to the vendor.

Exhibit 2: Examples of NARA-related Images Found on Media Cards



[redacted]

“National Archives”

“MPLS†”

“Tape Backup”

BlackBerry
National Archives
VC
114
34
24
TAPE BKUP
1. Location/Condition of Facility
2. Health Risk
3. Senior Leadership Buy-In
4. Storage for records - Physical
5. Security
6. No Vital Records Program
No COOP
7. Technology - backup situation
8. Multiple Record keeping processes
pipes
windows
HVAC
sprinkler

† Multi-Protocol Label Switching: A type of network NARA utilized before implementing the Trusted Internet Connection (TIC) service

Recommendations

We recommend NARA’s Chief Information Officer:

8. Develop and document policies and procedures on:
   a. Maintaining a complete and accurate inventory providing traceability to the user, phone number, physical location, and the dates the device was returned, disconnected, and wiped; and

  b. Mobile device retirement management process defining the steps needed to be performed, responsible party for each step, and the monitoring and reporting process.

9. Include in the device wipe process sanitization of all contents stored on media cards.

Management Response

Management concurred with the recommendations.

5. Strategy Needs to be Developed for Potential Mobile Device Portfolio Expansion

According to recent articles, BlackBerry's U.S. handset market share fell from 50% in 2009 to less than 3% in 2013, allowing its competitors to gain popularity in the market running on different operating systems. In November 2013, BlackBerry called off a tentative buyout and fired its Chief Executive Officer, heightening the uncertainty about the future of the company.[16] However, NARA currently has no other types of smartphones in its mobile device portfolio. This occurred because NARA has not established and implemented a detailed strategic plan for expanding its mobile device portfolio.

NIST SP 800-53 recommends, in order to limit harm from any given supplier in the supply chain, the organization employ a diverse set of suppliers from approved vendor lists with standing reputations in industry. NARA's ExchangeMyMail (EMM) system is a subsystem within the Google Apps system enabling users to send and receive NARA e-mail messages on their BlackBerry devices. NARA's Continuity of Operations Plan, dated January 31, 2014, states Google Apps are part of the NARANet baseline, which is inherently considered mission-critical for continuity purposes. Therefore, in order to minimize impact it may have on NARA’s continuity of operation in case BlackBerry devices become obsolete or there are other issues, NARA should (1) evaluate a variety of mobile devices for potential inclusion in its portfolio; and (2) be prepared to accommodate them through a reliable mobile device management (MDM) solution. A failure to do so may result in inability to secure and centrally manage mobile devices and data on them, jeopardizing the mobile computing and communication capability at NARA. When we brought this to management’s attention, they indicated NARA has recently formed a mobile device working group to expand mobile capabilities and acquire

[16] http://www.theguardian.com/technology/2013/nov/04/BlackBerry-fires-ceo-thorsten-heins-fairfax-bid-collapses

a MDM solution beyond the current MDM in place for BlackBerry devices. However, we found a formal strategy for the expansion has yet to be determined.

Recommendation

We recommend NARA's Chief Information Officer:

10. Develop a formal strategy to expand NARA's mobile device portfolio which includes the following:
    a. Evaluations of alternative mobile devices and MDM solutions; and
    b. Cost estimates, required resources, timelines, and technical recommendations for carrying out the expansion.

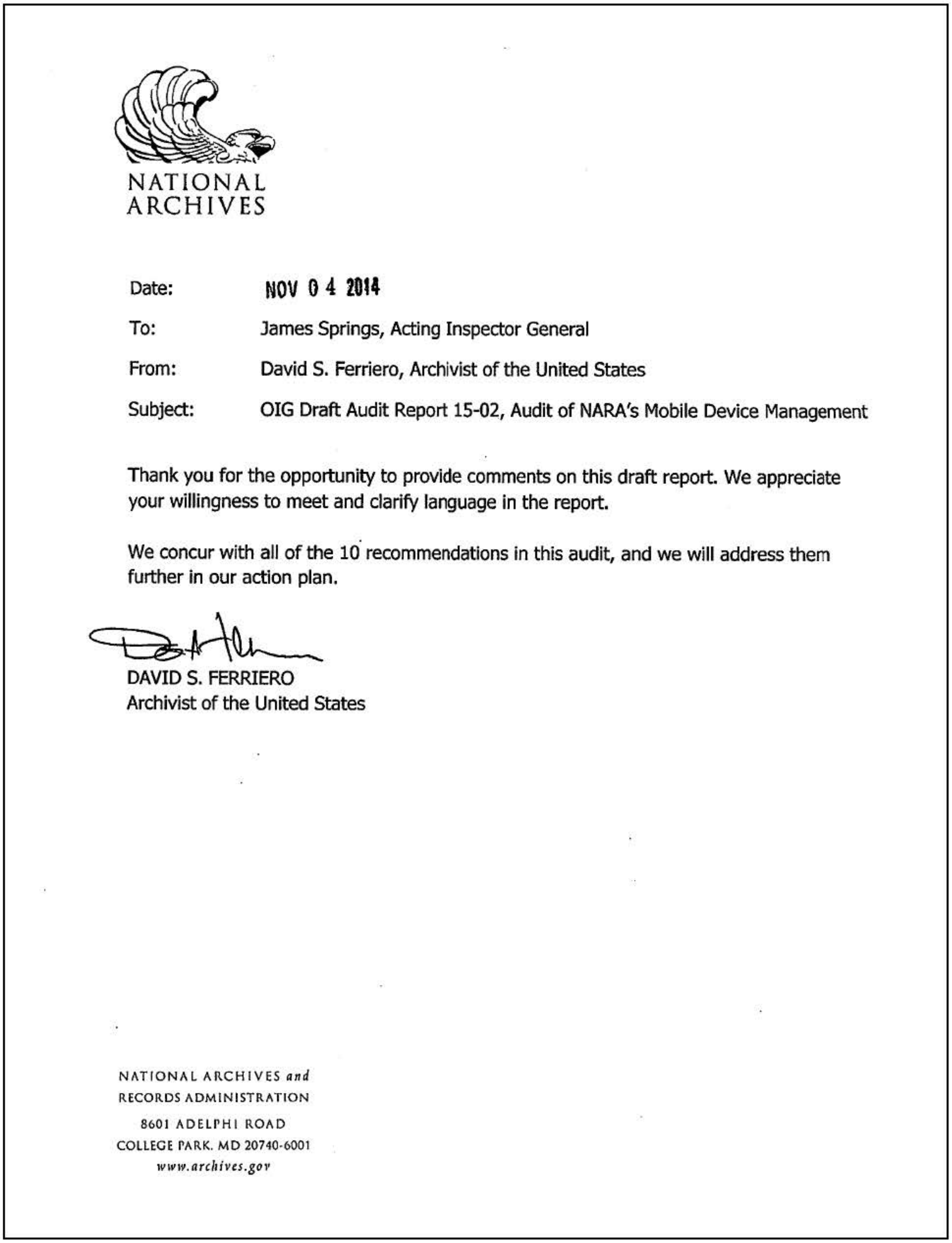
Management Response

Management concurred with the recommendation.

Appendix A – Acronyms and Abbreviations

BES	BlackBerry Enterprise Server
CIO	Chief Information Officer
DAS	Distributed Antenna System
DHS	Department of Homeland Security
DoD	Department of Defense
EMM	ExchangeMyMail
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IT	Information Technology
MDM	Mobile Device Management
MPLS	Multi-Protocol Label Switching
NARA	National Archives and Records Administration
NIST SP	National Institute of Standard and Technology Special Publication
NITTSS	NARA Information Technology and Telecommunication Support Services
OIG	Office of Inspector General
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIV	Personal Identity Verification
STIG	Security Technical Implementation Guides
TIC	Trusted Internet Connection
WSP	Wireless Service Provider

Appendix B - Management’s Response to the Report



NATIONAL
ARCHIVES

Date: NOV 04 2014

To: James Springs, Acting Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: OIG Draft Audit Report 15-02, Audit of NARA’s Mobile Device Management

Thank you for the opportunity to provide comments on this draft report. We appreciate your willingness to meet and clarify language in the report.

We concur with all of the 10 recommendations in this audit, and we will address them further in our action plan.

DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix C - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Chief Information Officer
Chief Innovation Officer
Chief, IT Service Branch