OFFICE *of*
INSPECTOR GENERAL
NATIONAL ARCHIVES

November 18, 2016

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs James Springs
Inspector General (OIG)

SUBJECT: *Audit of NARA's Management Control over Microsoft Access Applications and Databases*

Attached for your action is our final report, *Audit of NARA's Management Control over Microsoft Access Applications and Databases*. Based on your November 17, 2016 response to the draft report, we consider all recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed-upon corrective actions so that recommendations may then be closed.

As with all OIG products, we will determine what information is publicly posted on our website from the attached report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from your or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.

OFFICE *of*
INSPECTOR GENERAL
NATIONAL ARCHIVES

# Audit of NARA's Management Control Over Microsoft Access Applications and Databases

November 18, 2016

OIG Audit Report No. 17-AUD-04

# Table of Contents

# Executive Summary

*Audit of NARA's Management Control over Microsoft Access Applications and Databases*

OIG Report No. 17-AUD-04 November 18, 2016

## Why Did We Conduct This Audit?

NARA currently utilizes Microsoft (MS) Access 2007 and plans a rollout of MS Access 2013. However, these plans were put on hold due to concerns of the Chief Information Officer (CIO), who requested this audit. These concerns include lack of awareness of the number of Access applications/databases across the enterprise, locations of applications and underlying database, and security of the applications/databases. We conducted this audit to identify MS Access applications and databases in use across NARA, assess the security controls for those applications and databases, and determine whether NARA is appropriately positioned to accommodate and maintain the applications and databases and security controls after the planned MS Access upgrade to a newer version.

## What Did We Recommend?

NARA should evaluate the MS Access applications and databases used in each program office to determine their data sensitivity and mission-criticality, implement the security assessment process in accordance with their data sensitivity and mission-criticality, and develop a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system. We made 9 recommendation, if implemented will assist NARA in adequately preparing for its planned Microsoft Access upgrade.

## What Did We Find?

We identified a total of 1,800 MS Access applications/databases and found NARA is not appropriately positioned to accommodate the conversion from MS Access 2007 to 2013. They do not have appropriate operational and security controls in place to ensure uninterrupted functionality and data security. In addition, NARA does not have governing policy for authorizing and approving MS Access applications/databases. NARA's MS Access applications/databases currently bypass the agency-wide Authorization-to-Operate (ATO) process, and existing policies and procedures for protecting the security and integrity of data have not been adequately implemented on the applications/databases. These weaknesses exist primarily because NARA lacks effective management and internal controls to ensure its MS Access applications and underlying databases are authorized, secured and protect users' PII. Lack of effective controls jeopardizes NARA's ability to effectively and efficiently carry out critical functions and puts the agency at risk of causing substantial harm, embarrassment, or inconvenience to those whose PII is stored or maintained in its databases.

Also, the sustainability of the MS Access applications/databases after the planned upgrade is not ensured. We found mission-critical applications/databases contain programming tools that may prevent full conversion to MS Access 2013. Further, controls were not in place to ensure a backup of the previous system, or that user acceptance tests were completed. Without adequate user-acceptance testing of applications/databases and backup plans to prepare for potential post-conversion issues, some of the mission-critical systems, including those feeding NARA's official source of information, may not function as intended after the planned upgrade.

Additionally, during the audit, a database was deleted from the server by a NARA employee after the OIG requested supporting documentation on it. The user was not fully cognizant of their responsibility to cooperate with OIG's audit documentation requests. By deleting the database, the OIG was unable to observe and assess any data contained in, functionality of, or security controls over the deleted database. Although we determined the deletion was not due to a concealment of a fraud or employee misconduct, the deletion raised concern about employees' awareness of their responsibility to cooperate with OIG audit requests and abide by NARA's Records Schedule.

James Springs

**James Springs**
*Inspector General*

# Background

NARA's Office of Information Services (I) plans a rollout of MS Access 2013. However, these plans were put on hold due to concerns of the CIO, who requested this audit. These concerns include lack of awareness of the number of Access applications/databases across the enterprise, locations of applications and underlying database, and security of the applications/databases.

NARA currently utilizes MS Access 2007 for applications/databases after the previous Agency-wide upgrade. These applications/databases developed and utilized by NARA offices and organizations are currently not subject to the ATO process.

NARA's last MS Access conversion was a two-month project performed in 2009. This project was to convert the applications/databases that were in various older versions of MS Access to 2007. These older versions included 1997, 2000, and 2002. NARA contracted with a professional service firm to perform the conversion. The project originally identified approximately 15,000 MS Access applications/databases NARA-wide. However, after excluding ones not requiring conversion (multiple copies of same backups, etc.), the number of applications/databases subject to conversion ended up being only 1,320, approximately 9% of the total number of applications/databases identified.

The last conversion project included multiple testing procedures. The results of the converted applications/databases were generally well received by users.[1] However, users who had to develop a new MS Access application after the conversion had difficulty doing so because they were not familiar with the new version of MS Access. No guidance was provided to users on how to develop an application/database in the new version. In addition, the project was strictly for the conversion, and security of the applications/databases was not evaluated. Table 1below includes a summary of the applications/databases by each NARA organization converted to MS Access 2007 during the last conversion project. Appendix A of this report includes a summary of the Agency-wide survey conducted by NARA OIG between August and October 2015 to identify MS Access applications/databases subject to conversion. Appendix B includes a summary of the Triumfant[2] network scan report used to identify machines attached to NARA's network showing MS Access applications/databases.

[1] During the performance of this audit, we found one of the databases we sampled did not convert properly during the last conversion process and lost most of its functionality. See page 19 for more details.

[2] An information and integrity monitoring tool used for NARANet-hosted systems to detect unusual or unauthorized activities, conditions, or changes.

**Table 1: 2009 Conversion Project - Database Summary by Version and Organization**

| Version\Org[3] | NA | NH | NL | NR | NW | NF | N | Total |
|---|---|---|---|---|---|---|---|---|
| **2000** | 2 | 0 | 60 | 5 | 417 | 1 | 2 | 487 |
| **2002** | 7 | 3 | 331 | 227 | 199 | 3 | 32 | 802 |
| **1997** | 0 | 0 | 4 | 0 | 17 | 0 | 0 | 21 |
| **Unknown** | 0 | 0 | 2 | 0 | 8 | 0 | 0 | 10 |

[3] In 2011, NARA underwent a series of reorganization efforts, resulting in changes in the organization codes. Since the conversion occurred prior to the reorganization, this table reflects the organization codes before the reorganization. See NARA Directive 101, Appendix B – *NARA Organization Codes* for an old to new organization code crosswalk.

# Objectives, Scope, Methodology

The objectives of this audit were to identify MS Access applications/databases in use across NARA, assess the security controls for those applications/databases, and determine whether NARA is appropriately positioned to accommodate and maintain the applications/databases and security controls after the planned MS Access upgrade.

To accomplish our objectives we conducted a survey encompassing all NARA organizations to identify and obtain preliminary information on the MS Access applications/databases used by the organization. We identified 1,800 applications/databases through the agency-wide survey[4] and selected a judgmental sample of 20 applications/databases based on factors including mission-criticality, data type, record count, number of users, and complexity of the application/database. This judgmental, non-statistical sample cannot be projected to the intended population. As part of the reviews, we conducted meetings with the representatives of NARA organizations and obtained relevant documentation[5] to learn more details about the sampled applications/databases. This information included the purpose, type of data maintained or processes used, security controls, and any concerns users had regarding security and sustainability of the application/database in the current and future versions of MS Access. Table 2 below lists the applications and database sampled for our review.

**Table 2: MS Access Applications/Databases Sampled**

| Office Symbol | Office | Name of Application/Database |
|---|---|---|
| AC | Office of the Chief Records Officer | Control and Tracking System (CATS) |
| AFN | National Personnel Records Center (NPRC) | Desert Shield / Desert Storm (OASIS) |
| AFO | Federal Records Center Program | P23/E23 |
| ANDC | National Declassification Center | Onestop Unclass New |
| B | Business Support Services | Seattle File Plan |
| F | Office of Federal Register | 2012 Election Info |
| H | Office of Human Capital | HTL Tracking |
| IXO | Office of Information Services Digital Preservation Operations Branch | APS Job Loc |
| LL | Center for Legislative Archives | LL Reference Topic Log |
| LM | Legislative Archives, Presidential Libraries, and Museum Services – Presidential Materials Division | Sampled Mail |
| LP | Office of Presidential Libraries – Central Office | NL211 |

[4] Details about the survey results are discussed in Appendix A of the report.

[5] Documentation we reviewed included user manuals, screenshots, sample forms and reports, data extracts, Standard Operating Procedures (SOPs), and contracting documents.

**Table 2: MS Access Applications/ Databases Sampled (continued)**

| Office Symbol | Office | Name of Application/Database |
|---|---|---|
| LP – DDE | Dwight D. Eisenhower Presidential Library | LS20A Register |
| LP – LBJ | Lyndon B. Johnson Presidential Library | Museum Loan LB Access |
| LP – RNL | Richard Nixon Presidential Library | Public Vaults |
| NGC | General Counsel | Mandatory Declassification Review (MDR) Appeals |
| RD | Research Services Access Coordinator | Pull Database |
| SP | Strategy and Performance | Internal Control Program (ICP) |
| SP | Strategy and Performance | NARAStat |
| V | Office of Innovation | Central Table |
| V | Office of Innovation | Still Image Job Log |

We obtained and reviewed lists of the NARANet[6] users who have access to the applications/databases from NARA Information Technology & Telecommunication Support Services (NITTSS) to determine if their access to the application or database was in accordance with their job responsibilities. We also interviewed the employee in charge of the previous MS Access conversion project performed in 2009, and reviewed related documentation to gain an understanding of the last conversion process and issues NARA faced during the conversion.

We also reviewed applicable federal requirements, NARA policies and procedures, and National Institute of Standards and Technology (NIST) guidance and industry-best practices, including:

- The Privacy Act (5 U.S.C. § 552a(e)(9)-(10);
- Office of Management and Budget (OMB) Memorandum M-06-15, *Safeguarding Personally Identifiable Information*;
- Inspector General Act of 1978, as amended;
- Title 18 U.S.C., Chapter 73, Section 1516, *Obstruction of Federal Audit*;
- NARA Directive 1201, *Audits of NARA Programs and Operations*, dated May 15, 2012;
- NARA Directive 1608, *Protection of Personally Identifiable Information (PII)*, dated August 6, 2009;
- *NARA IT Security Requirements*, Version 6.0, dated November 10, 2014;
- National Institute of Standard and Technology Special Publication (NIST SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013;
- Federal Information System Controls Audit Manual (FISCAM), dated February 2009; and
- SANS Institute Whitepaper, *Making Database Security an IT Security Priority*, dated November 2009.

This performance audit was conducted at Archives II in College Park, Maryland, in accordance with generally accepted government auditing standards between July 2015 and July 2016. The

[6] NARA's unclassified computer network providing access to NARA's intranet, email, and the Internet.

generally accepted government auditing standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Jina Lee, Senior IT Auditor.

# Audit Results

## Finding 1. NARA Lacks Adequate Management Control over MS Access Applications and Databases.

We found NARA is not appropriately positioned to accommodate the conversion from MS Access 2007 to 2013. Specifically, we noted applications/databases did not have user authentication, audit logging, differentiated access level, or restricted folder access; and Personally Identifiable Information (PII) was not adequately protected. In addition, NARA does not have governing policy specifically for authorizing and approving MS Access applications/databases. NARA's MS Access applications/databases currently bypass the agency-wide Authorization-to-Operate (ATO) process, and existing NARA policies and procedures for protecting the security and integrity of data have not been adequately implemented on the applications/databases. These weaknesses exist primarily because NARA does not have a comprehensive, systematic process to determine when a MS Access application or database should be included in its system inventory, which led to lack of effective management and internal controls to ensure its MS Access applications and underlying databases are authorized, secured, and protect users' PII. According to FISCAM, the entity cannot effectively manage information security controls across the entity without maintaining a complete, accurate, and up-to-date inventory of its systems. It also states the inventory is necessary for effective monitoring, testing, and evaluation of information security controls, and to support IT planning, budgeting, acquisition, and management. Lack of effective controls jeopardizes NARA's ability to effectively and efficiently carry out critical functions and puts the agency at risk of causing substantial harm, embarrassment, or inconvenience to those whose PII is stored or maintained in its databases.

<u>User Accountability and Data Integrity Not Ensured</u>

Among the 20 applications/databases sampled, we found user accountability and data integrity were not ensured on at least nine. Four of the nine, MDR Appeals, LL Reference Topic Log, OASIS, and Pull Database, contained PII.[7] The other five applications/databases included Control and Tracking System (CATS); HTL Tracking; Onestop Unclass New; Seattle File Plan; and Still Image Job Log. The following issues were noted on each of the five applications/databases:

- CATS database is used by the office of the Chief Records Officer (AC), primarily within the Records Appraisal and Agency Assistance (ACRA) unit to track pending federal

[7] Details regarding the type of and issues related to the PII contained in these databases are discussed later in the report.

agency records schedules,[8] media-neutral notifications, and internal disposals. According to the ACRA representative who maintains the database, this is a mission-critical database to the office because it tracks the schedules submitted by federal agencies for review and approval by NARA, which is the core work of the ACRA unit. Having proper controls to ensure data is secure and accurate is essential to successfully carrying out the mission. We found the database was not adequately secured from unintended data addition, modification, or deletion. According to the ACRA representative, approximately 50 employees, consisting of all of the ACRA employees and a few managers in AC, use the database to perform their job responsibilities. We noted the folder where the database resides is not properly restricted and over 250 individuals have access to the database. Moreover, although the ACRA representative who maintains the database is the only user who requires administrator access to the database, the access level is not differentiated by user.  CATS contains all data within itself as tables, and all users have the same read and write access to the database, indicating  all of the users can view, modify, and delete any data in the tables. Further, CATS is not password-protected, and user activity is not logged.  In the event of unauthorized changes to the data, it would be difficult to identify the change or the user who made the change.

- HTL Tracking is used by the Human Capital Office (H)'s Labor/Employee Relations and Performance and Awards Branch (HPP) to track and update personnel occurrences in the respective program areas. The information collected includes the case type, date of contact, parties involved, and a running plan of action. In addition to personnel matters, HPP staff track instances of advice and guidance with NARA customers and union-related communication (grievances, unfair labor practices, requests for information, and notifications). Although this database is password-protected, the password is shared among all twenty users and does not periodically change. No track changes or audit logging is enabled on the database.  If erroneous data entry or data removal takes place, there would not be a way to hold the user accountable for the action. A HPP representative agreed it might be a good idea to lock some rows to prevent accidental data loss/change for pertinent information.

- Onestop Unclass New is used in the National Declassification Center (ANDC) and serves as a bridge between the Holdings Management System (HMS) and Archival Declassification, Review and Redaction System (ADRRES) to ensure ANDC has a full understanding of the status of projects being tracked in either system. It also allows ANDC to track all of its workflow steps for any project being handled for system declassification processing. In addition, it provides one mechanism for all key production

[8] Federal agency records schedules are generally submitted via the Electronic Records Archives (ERA); however, agencies that are granted an exception use the SF-115 form, *Disposition of Federal Records*. These schedules provide legal authority to federal agencies for disposal of records.

reporting on ANDC's declassification activities, including custom-designed tracking reports and Performance Management and Reporting System (PMRS) inputs. In January 2016, the Structured Query Language (SQL) back-end tables were implemented to the database through an Open Database Connectivity (ODBC) setting. This enabled the audit logging capability, where user activity can be tracked through their user IDs. According to an ANDC representative, each user has his/her own user ID which is needed to track user activity. We found the password to the database is shared among all users (15 to 20 users), and the password is not periodically changed.

- Seattle File Plan is a local files plan database for NARA’s Seattle facility that identifies the file code, description, and disposition authority for each type of record the Seattle office creates and maintains. The database does not contain any PII or otherwise sensitive information. However, it contains numerous tables, queries, forms, and reports to support the administrative functions such as determining where to file documents, printing labels to affix to file folders, and generate reports related to the files plan as necessary for senior staff in the office. The database is stored on the shared drive for the Seattle facility, and the folder where it resides is not restricted further. According to the primary user, no more than four staff use the folder.  However, we found a total of 37 individuals had access to the folder as of April 2016. This database is not password-protected, therefore all individuals who are granted access to the shared drive could freely access any data, queries, forms, and reports included in the database. During our interview with the primary user of the database, she indicated her preference for the database to be password-protected in order to prevent any intentional or unintentional data removal or manipulation.

- Still Image Job Log is used by the Office of Innovation’s (V’s) Digitization Services Branch (VIS) to track imaging jobs through their various stages of completion (pending, in-progress, completed). Lab staff keys in data regarding the material type, requesting work unit, job instructions, assigned technician, number of completed image files created for the job, as well as any other pertinent details. Once the original materials and project deliverables are retrieved by the requesting unit, that information is recorded in the database to finalize the job. Although some of this data can be found in HMS, not all projects that come to the lab, or services provided by the lab are represented in HMS. The database allows VIS to record all projects in one location. This database is a critical tool for VIS to perform its mission of record imaging as it provides a comprehensive view of all imaging projects, whether or not they are represented in HMS. Assuring data integrity for this database is important in order to accurately track and efficiently respond to all imaging requests. We found this database is located on V’s shared drive where approximately 500 individuals have access, and is not password-protected. However, a VIS representative indicated only two employees are required to use the database to accomplish their job responsibilities. Audit logging is not enabled on this database. Since it's also accessible to all individuals who are granted access to the shared drive, this database is at a risk of inappropriate use, modification, or deletion of data by unintended users.

Personally Identifiable Information (PII) is not adequately protected

Among the 20 applications/databases in the sample, we found four databases contained PII as shown below in Table 3.

**Table 3: Types of PII Contained in Databases**

| **Office Symbol** | **Office** | **Database Name** | **Type of PII** |
|---|---|---|---|
| AFN | National Personnel Records Center (NPRC) | Desert Shield / Desert Storm (OASIS) | Veterans' names and social security numbers |
| LL | Center for Legislative Archives | LL Reference Topic Log | Researchers' names contact information (phone numbers and email addresses) |
| NGC | General Counsel | MDR Appeals | Requestor's names and contact information |
| RD | Research Services Access Coordinator | Pull Database | Names of staff member performing the pull and refiles; names and photos of researchers |

Based on the description of the databases, we found it was appropriate for the databases to contain such information to serve their purposes. However, user authentication to access information in the database was not in accordance with NARA Directive 1608, which requires electronic files containing PII to be password-protected when maintained within the Agency's network boundaries. It also requires the CIO to conduct periodic risk assessments to identify areas of privacy-related vulnerabilities and risks. Noncompliance with the policy occurred because NARA does not have a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system. The failure to include MS Access applications/databases in system categorization resulted in them bypassing the security assessment process described in NARA's Enterprise Architecture, putting the agency at risk of causing substantial harm, embarrassment, or inconvenience to those whose PII is stored or maintained in its databases.

The following describes the issues noted on each of these databases.

- Desert Shield/Desert Storm (OASIS) is a read-only registry and finding aid tool providing a list of all soldiers who participated in Operations Desert Shield and Desert Storm (aka. The first Gulf War). This system is used by the NPRC employees to determine if a veteran participated in the Operations when such information cannot be found in the veteran's Official Military Personnel File (OMPF). Users of this registry can search for a veteran by either the name or social security number. Upon completion of a search, a user can populate a report containing PII such as the name and social security number as well as the branch of service, component, and active duty period. We found users are not required to enter a password to access the registry and perform the search.

According to the Supervisory Management Analyst at the NPRC, only the system administrators have read and write access to the front-end application and back-end tables, both in MS Access. Other NPRC employees' access to the front-end application is granted through the access request form submitted to the helpdesk by the new user's supervisor and is limited to read-only. We found once the users log on to the Novell environment, a separate password is not required to access the registry, which includes PII. This is not in accordance with NARA Directive 1608, which requires any PII-containing files to be password-protected when maintained within the boundaries of the agency network. According to FISCAM, encryption is one of the technologies used to control sensitive data. Although this database contains highly sensitive data such as veterans' social security numbers, it was not encrypted in transmission or storage, making the data vulnerable to losing confidentiality if hackers break into the database.

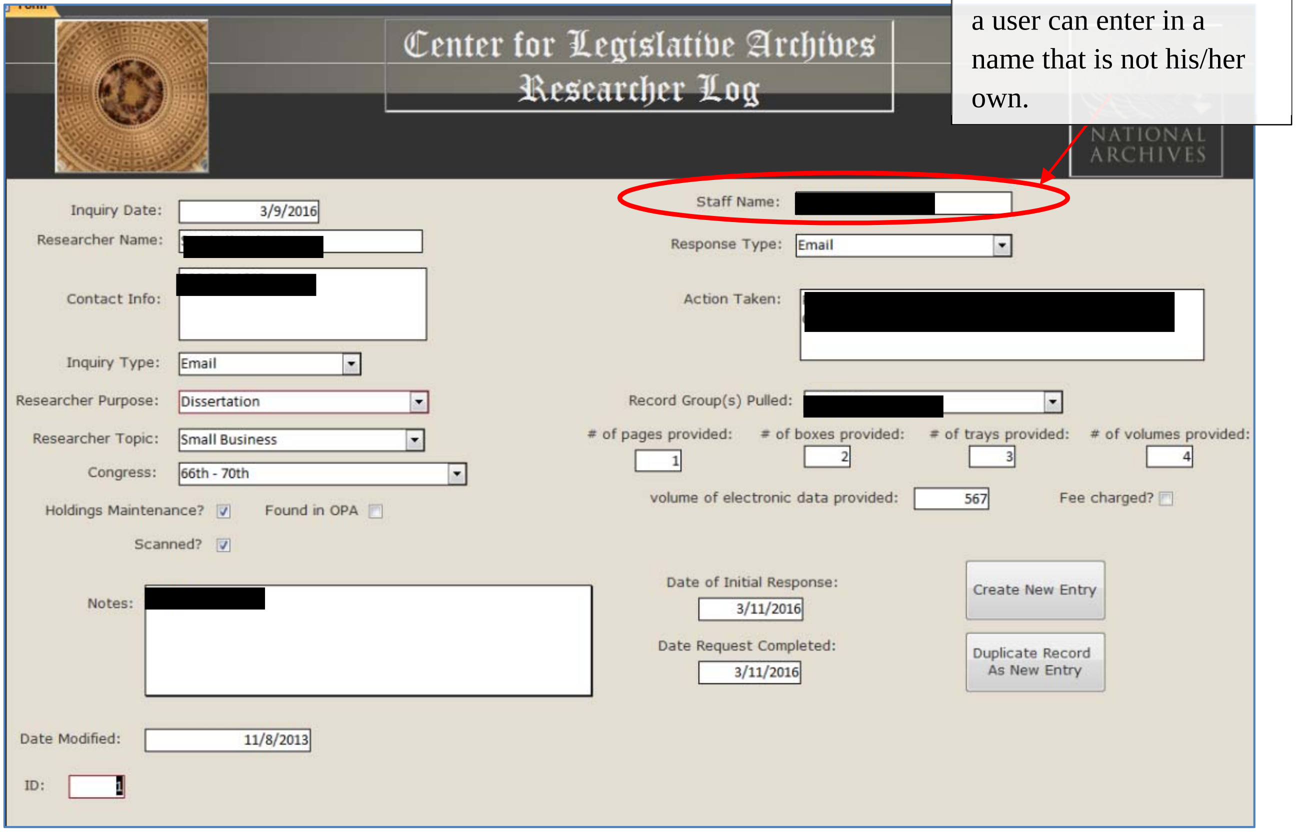
- LL Reference Topic Log is used by the Center for Legislative Archives (LL) employees to track researcher requests in order to avoid duplication and make future transactions more efficient. After the office responds to a reference request, it makes an entry in the log noting how the request came to the office (email, letter, call, walk-in, etc.) and how many boxes it pulled or pages it supplied to respond to the request. This is a split database between the front-end application and back-end tables, both of which are in MS Access. The front-end application is installed on users' desktops and the back-end tables reside on the office's shared drive on the network. According to the POC for the database, there are 11 employees who use the database; however, one password is shared among all users, and the password is not routinely changed. Also, the name of the approved staff entering the transaction is not automatically populated on the data entry page of the front-end application. If a user enters in a name that is not his or her own, it would be difficult to detect who actually entered in the incorrect name.

  Further, the back-end tables are not password-protected.  Anyone who has access to the office's shared drive can access, modify, and delete any information in the tables. According to the list of members who have access to the file location provided by NITTSS, 23 individuals had access to the location as of April 2016. As previously mentioned, only 11 staff need to use the database. The database is not password-protected, and is accessible to those whose roles and responsibilities do not require access. In addition, audit logging is not enabled on the database.  If data is inappropriately added, modified, or deleted, it would be difficult to detect and hold the user accountable for the action.

Figure 1 below shows the data entry page of the front-end application of the database where the user can enter in information such as the inquiry date, researcher's name and contact information, staff performing the transaction, dates of initial response and request completed.

**Figure 1: LL Reference Topic Log Data Entry Page**

Staff name is not automatically populated; a user can enter in a name that is not his/her own.



Center for Legislative Archives
Researcher Log
NATIONAL ARCHIVES
Create New Entry
Duplicate Record As New Entry

Inquiry Date: 3/9/2016

Researcher Name: [redacted]

Contact Info: [redacted]

Inquiry Type: Email

Researcher Purpose: Dissertation

Researcher Topic: Small Business

Congress: 66th - 70th

Holdings Maintenance? ☑ Found in OPA □

Scanned? ☑

Notes: [redacted]

Date Modified: 11/8/2013

ID: 1

Staff Name: [redacted]

Response Type: Email

Action Taken: [redacted]

Record Group(s) Pulled: [redacted]

# of pages provided: 1 # of boxes provided: 2 # of trays provided: 3 # of volumes provided: 4

volume of electronic data provided: 567 Fee charged? □

Date of Initial Response: 3/11/2016

Date Request Completed: 3/11/2016

- MDR Appeals is a tracking system accounting for mandatory declassification review appeal requests that might come from any of the offices within NARA that contain National Security Information (NSI). This database does not contain NSI itself because it is maintained with the office that owns the record. However, it contains PII such as the requestor's name and contact information including the mailing address, email address, and phone numbers. According to the Freedom of Information Act (FOIA) & Privacy Act Officer in NGC, only three to five individuals in the office use the database. However, all NGC employees have access to the database as it resides on NGC's shared drive and is not password-protected. According to NITTSS, as of April 2016, 15 members were granted access to the shared drive.

- Pull Database tracks pull transactions in the Textual Research Rooms in Archives I and Archives II and includes information such as the scheduled pull time, researcher names and their arrival/departure times, staff member performing the transaction, refiles, and staff member performing the refile. It also contains researchers' photos.[9] Employees can access the database via either the shared kiosks or via personal workstations (if the client is installed on them). Users who have the client installed on their personal workstations have an account on the server and log in as themselves. However, users who only use the client on the shared kiosks log in using a shared Novell ID. According to the employee who maintains the database, he originally suggested each person use his/her own Novell account in order to use the database, which would be the only way to implement audit logging of who accessed the system. According to the staff, his suggestion was overruled by his manager due to the time it takes to log out and log back into the system.

In addition, there appeared to be a misunderstanding between Research Services and Information Security concerning approval of using a shared login. The Research Services representative believed the shared Novell login was created with approval from NARA's Information Security. However, our inquiry with an Information Security representative revealed what was approved was a shared local Windows account to log onto the workstation, and not a shared Novell login. NARA's Information Security currently sees the shared Novell login to access a database containing PII as a problem, as it violates NARA Directive 1608.

Further, we found the server where the back-end database resides, in SQL, had not been backed up. A backup request form was originally completed when the new Researcher Registration Service (RRS) server, where the database resides, went online around April 2015. However, the backup request was not adequately followed up, and the server backup did not start until June 2016, five months later. The backup of the server started during the course of this audit as a result of our inquiry on whether the database was being backed up. A failure to ensure servers containing critical information are backed up may cause inconvenience and inability to carry out NARA's mission in case data is lost, corrupted, or undesirably changed on the server.

The Privacy Act requires each agency to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records, and to protect against any anticipated threats or hazards to their security and integrity. In addition, NARA Directive 1608 states if users collect, maintain, handle, access, or disseminate PII in the course of performing their official duties, they must password-protect electronic files containing PII when maintained within the boundaries of the agency network.

[9] Researcher photos are stored in the back-end database, where only the administrators have access; however, staff members can view the displayed image via the local machines.

Further, NIST SP 800-53 states, organizations may require unique identification of individuals in a group account (e.g. shared privileged accounts) or for detailed accountability of individual activity. NARA's Enterprise Architecture states for all data, NARA's Information Technology (IT) staff shall: (a) assess the security controls in the information system and its environment at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; (b) produce a security assessment report that documents the results of the assessment; and (c) provide the results of the security control assessment to the authorizing official. According to the FISCAM, controls over sensitive system resources are designed to ensure confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage.

## Recommendations

Management control over NARA's MS Access applications/databases, including the security and data integrity controls, needs significant improvement. We recommend the Chief Information Officer, in conjunction with each program office:

**Recommendation 1:** Evaluate the MS Access applications/databases used in each program office to determine their mission-criticality to NARA and/or each program office.

Management Response

NARA concurs with this recommendation. Information Services will develop a phased plan for working with each program office to evaluate the offices' MS Access applications/databases used in each program office and determine their mission-criticality to NARA and/or each program office. The work to evaluate and disposition over 700 databases for compliance with operational and security SOPs will take a minimum of 2 years, not to mention the evaluation of over 1000 other databases that were identified in the NARA environmental scan. Resources will be requested through a Freeze Exception Request for this work.

*Target Completion Date*: Phased Plan, June 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved pending completion of the corrective actions identified above.

**Recommendation 2:** Implement the security assessment process as described in NARA's Enterprise Architecture to those applications/databases determined critical to carrying out NARA's or program offices' missions from Recommendation 1.

Management Response

NARA concurs with this recommendation. Concurrent with implementation of the phased plan for evaluating the databases, security assessments will be conducted on applications/databases determined to be mission-critical systems as well as those determined to store PII. The guidance developed for compliance with operational and security SOPs discussed in Recommendation 5 will be used to review the databases. As with Recommendation 1, this work will require additional staff and at least 2 years to accomplish.

*Target Completion Date*: As defined in the Phased Plan developed in Recommendation 1.

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 3:** Develop and implement a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system.

Management Response

NARA concurs with this recommendation. Information Services will develop a FISMA System Inventory Standard and implement a process for determining when a MS Access application or database should be recognized as an IT system.

*Target Completion Date*: June 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 4:** Determine all MS Access databases containing PII and ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.

Management Response

NARA concurs with this recommendation. MS Access databases containing PII will be among the first to be examined in the Phased Plan developed for Recommendation 1 to ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.

*Target Completion Date:* The phased plan delivered in Recommendation 1 will provide the target date for completing the analysis of MS Access databases containing PII. Information Services estimates the analysis will be finished by December 31, 2017.

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 5:** Develop and implement a process for future MS Access applications/databases created by program offices, including notification to and approval from the Office of Information Services for those that are mission-critical and/or contain PII or otherwise sensitive information.

Management Response

NARA concurs with this recommendation. Information Services will incorporate database requirements within the IT governance process and directive. When an office identifies a database requirement, it will first develop a business need statement as defined in the IT governance process. That process will determine a solution that is sustainable by the OCIO.

*Target Completion Date*: April 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

## Finding 2. Sustainability of MS Access Applications/Databases Not Assured.

The sustainability of the MS Access applications/databases after the planned upgrade is not ensured. We found mission-critical applications/databases in the sample contain programming tools that may prevent full conversion to MS Access 2013. During NARA's last MS Access conversion in 2009, a database which was heavily dependent on macros and VBA lost most of its functionality after the conversion. NARA did not have a full understanding of the purpose and complexity of MS Access applications/databases created and utilized by different organizations. Further, controls were not in place to ensure a backup of the previous system, or that user acceptance tests were completed. FISCAM states, in the implementation phase, the entity configures and enables information system control features, tests the functionality of these features, installs the system, and tests system prior to placing it into operation to ensure that it meets all required security specifications. In addition, for data requiring moderate or high integrity NARA's Enterprise Architecture requires the NARA System Owner to retain older versions of baseline configurations to support rollbacks. Without adequate user-acceptance testing of applications/databases and backup plans to prepare for potential post-conversion issues, some of the mission-critical systems, including those feeding NARA's official source of statistical management information, may not function as intended after the planned upgrade.

<u>Mission-Critical Applications/Databases</u>

Our Agency-wide survey revealed at least 251 of 740 MS Access applications/databases contain programming tools such as macro and VBA.[10] Among the 20 applications/databases in the sample, 10, or 50%, had programming tools such as macros or VBA. These programming tools serve various purposes, including running a series of queries, populating reports, and providing data to PMRS, NARA's official source of statistical management information. We determined at least 8 of 10 applications/databases serve critical missions for the organization. Table 4 below describes the main purposes of the 8 applications/databases.

**Table 4: Mission-critical Applications/ Databases in the Sample Containing Programming Languages**

| Office Symbol | Office | Application/Database Name | Purpose |
|---|---|---|---|
| AC | Office of the Chief Records Officer | CATS | To document the registration and processing of SF-115s submitted by agencies or developed by NARA Archivists. |
| AFN | National Personnel Records Center | OASIS | To make a determination of veterans participation in the Desert Shield / Desert Storm Operation when such information cannot be found in the veteran's OMPF record. |

[10] Appendix A includes the result of the agency-wide MS Access Applications and Data survey NARA OIG conducted between August and October 2015.

**Table 4: Mission-critical Applications/Databases in the Sample Containing Programming Languages (continued)**

| Office Symbol | Office | Application/Database Name | Purpose |
|---|---|---|---|
| AFO | Federal Records Center Program | P23/E23 | To identify errors that must be corrected before data is migrated from ARCIS to ERA, including incomplete or inaccurate inclusive dates, container types, or disposition authorities for records. |
| ANDC | National Declassification Center | Onestop Unclass New | To connect data from HMS and ADDRES to ensure the Office has a full understanding of the status of declassification projects being tracked in either system. |
| LP | Office of Presidential Libraries | NL211 | To track the receipt and completion dates of written requests about holdings in LP, in order to ensure it meets NARA's 10 working day requirement to respond to the requests. |
| RD | Research Services Access Coordinator | Pull Database | To track pull transactions in the Textual Research Rooms in Archives I and Archives II and includes information such as the scheduled pull time, arrival time, staff member performing the transaction, refiles, and staff member performing the refile. |
| SP | Strategy and Performance | ICP | To allow program owners to review his or her program and summarize its condition from the standpoint of internal controls. |
| SP | Strategy and Performance | NARAStat | To provide quarterly reporting to managers to review agency status and progress. |

During the last MS Access conversion, one of the eight databases noted above (CATS), did not properly convert due to macros embedded in the application/database. CATS was heavily dependent upon macros and other codes, and there was no manual produced to document the construction of CATS as it had evolved over time. The office did not have the resources to rebuild the CATS database as it operated in earlier versions of MS Access.  The database had been corrupted such that it no longer functioned properly in the previous version of MS Access. The only documentation that could be created was screen captures of list of forms, reports, queries, and macros. As a result, a new, simplified database had to be created in MS Access 2007 that only had registration, closeout, and reporting functionality.  This limitation caused a loss of workflow tracking in one centralized location.

PMRS Reporting

PMRS is NARA's official source of statistical management information. It is a data warehouse application that presents data aggregated from offices throughout the agency to provide managers with consolidated view of data that covers many of the functions and operations of the agency (e.g. records processing, hiring, etc.). The data warehouse stores more than 8.4 gigabytes of data.

PMRS has two primary functions, (1) loading the data warehouse and (2) publishing its contents. The load process is done monthly through a number of batch processes pulling data from approximately 76 sources. The publication process is completed through a web-based self-service analytical tool, currently Databeacon. Unless the source database is small enough to be ingested wholly into PMRS, source data is extracted from the source into a file suitable for sending into the warehouse. Currently, the only file formats used for input files are MS Access (52 files, 91%), text files (four files, 7%), and MS Excel (one file, 2%).

The data sources include paper report sources, whole-source inputs, PMRS-pulled extracts, supplier-pulled extracts, and PMRS-hosted source systems. Paper report sources are used when figures needed do not exist in a machine-readable format. Whole-source inputs are used when the source system is small enough that the source file is itself the input file. PMRS-pulled extracts are input files that are extracted by the PMRS Operator by reaching across the NARANet to read the source system. Supplier-pulled extracts are the files extracted by the supplier, and PMRS has no direct visibility into the source database. PMRS-hosted source systems reside in the same SQL server with the PMRS data warehouse and have MS Access 2007 front-end databases, enabling users to view or input data. The front-end databases are available to users via either ZENworks[11] or a preinstalled copy of the database on users' desktops.

We found 6 of the 20 applications/databases sampled, or 30%, are used to feed PMRS. Table 5 below lists the six applications/databases and their source file type (paper report, whole-source, PMRS-pulled extracts, supplier-pulled extracts, or PMRS-hosted source system). At least 164 of 740 applications/databases or 22%, for which survey responses were received were identified to be data sources for NARA's critical strategic monitoring activities, including PMRS.

[11] An application enabling users to open the user's local copy of the database on his/her desktop as a single-user database; all data is stored on the SQL server where PMRS data warehouse resides.

**Table 5: Applications/Databases Used to Feed PMRS in the Sample**

| Office Symbol | Office | Application/Database Name | Source File Type |
|---|---|---|---|
| AC | Office of the Chief Records Officer | CATS | PMRS-pulled extracts |
| ANDC | National Declassification Center | Onestop Unclass New | PMRS-pulled extracts |
| LL | Center for Legislative Archives | LL Reference Topic Log | PMRS-pulled extract |
| LP | Office of Presidential Libraries | NL211 | Whole-source input |
| RD | Research Services Access Coordinator | Pull Database | PMRS-pulled extracts |
| SP | Strategy and Performance | ICP | PMRS-hosted source system |

Currently, paper report sources and supplier-pulled extracts heavily involve manual processes, which leaves room for human error. As stated above, in some cases, the PMRS Operator has no knowledge of what the sources are for supplier-pulled extracts. NARA has recently awarded a contract to design, develop, test, train, and put into production an enterprise data warehouse capability replacing the existing PMRS and its infrastructure (PMRS 2.0). NARA's Office of Strategy and Communication (SP) understands the need to test the current and future versions of PMRS and the various pulls from different sources to determine how they work with MS Access 2013. The Office does not see the need to change the pull methods with the MS Access upgrade; however, if PMRS 2.0 is to become a more comprehensive system than the current version, it could affect the way the system takes in data.

## Recommendations

We recommend the Chief Information Officer, in conjunction with each program office:

**Recommendation 6:** Identify all MS Access applications/databases containing programming languages and/or are source data for PMRS.

Management Response

NARA concurs with this recommendation. The phased plan developed in Recommendation 1 will include a review process for those applications/data bases containing programming languages and/or are source data for PMRS. Information Services, in conjunction with each program office, will evaluate the MS Access applications/databases used in each program office to evaluate and list the programming languages used for all the MS access applications/databases and create a list of current sources that feed data into PMRS.

*Target Completion Date*: June 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 7:** Ensure availability of rollback versions of applications/databases in the event they don't properly convert to MS Access 2013.

Management Response

NARA concurs/does not concur with this recommendation. It is not a given that the eventual migration for these databases will be to a current version of MS Access. The need for the database will be matched against the tools currently in the IT portfolio. If no appropriate tool is identified, an upgrade to MS Access will be considered. Regardless of selected tool, conversion planning will incorporate the need for rollback versions of applications/databases. Information Services, in conjunction with each program office, will create and provide procedures for maintaining proper version controls and backups to ensure that the previous versions of MS Access applications/databases are preserved securely for analyzing and addressing the future conversion and data related issues.

*Target Completion Date:* June 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

We recommend the Chief of Management and Administration:

**Recommendation 8:** Consider standardizing PMRS' source pull method in order to minimize potential for human error when developing PMRS 2.0.

Management Response

NARA concurs/does not concur with this recommendation. The Chief of Management and Administration, in conjunction with Information Services and each program office, will consider standardizing PMRS's source pull method and will provide documentation and justification of their decision.

*Target Completion Date:* March 31, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

## Finding 3. Employee Cooperation with OIG Requests.

During the course of this audit a database was deleted from its server by a NARA employee after the OIG requested supporting documentation concerning the database. The user was not fully cognizant of their responsibility to cooperate with OIG's audit documentation requests. By deleting the database, the OIG was unable to observe and assess any data contained in, functionality of, or security controls over the deleted database. NARA Directive 1201, *Audits of NARA Programs and Operations*, requires executives, staff directors, and managers to ensure staff fully cooperate with the OIG, including providing access to all information requested by auditors. In addition, the Inspector General Act of 1978 (IG Act), as amended, states each Inspector General is authorized to have access to all records, reports, audits, reviews, documents, papers, recommendations, and other material available to the applicable establishment which relate to programs and operations with respect to which that Inspector General has responsibility. Although we determined the deletion was not due to a concealment of a fraud or employee misconduct, the deletion raised a concern about employees' awareness of their responsibility to cooperate with OIG audit requests and abide by NARA's Records Schedule.

We requested the Richard Nixon Presidential Library (RNL) representative complete a survey for one of the MS Access databases that was not included in the original survey response for the Library. As opposed to completing the request, the representative deleted the database.  The representative indicated they deleted the database because they believed it would be quicker than completing the survey. After learning of the deleted database, we requested the backup be restored on the server.  At the time of the request, the backup file had already been discarded since it had passed the retention period. The employee was not fully cognizant of his responsibility to cooperate with OIG's audit requests. By deleting the database, the OIG was unable to observe and assess any data contained in, functionality of, or security controls over it.

The RNL representative later stated they were able to find two older versions of the database, one in MS Access 2000 and another in 2002 and provided a copy of each version. They contained the same number of records in each version, and the data in the tables appeared to be identical and free of PII or otherwise sensitive information. The database contained information such as document title, document date, repository (all Presidential Libraries or Projects), general records type, citation, and whether an image exists for the document exhibited in the Public Vaults. According to the RNL representative, since they joined the Library in 2008, they had not used the database or heard of any other staff using it. They also stated based on the name of the file, they believed it was only used to record information about documents exhibited in the Public Vaults, possibly when that exhibition was new in 2003. However, since the requested database, which was in MS Access 2007, was no longer available, we were unable to determine the accuracy of the representative's statement.

The NARA Records Schedule provides mandatory instructions (“disposition instructions”) to all NARA staff regarding how to maintain the agency’s operational records and what to do with them when they are no longer needed for current business. The disposition instructions state whether individual series of records are “permanent” or “temporary”, as well as how long to retain the records. Records with historical value, identified as “permanent” are transferred to the National Archives. All other records are identified as “temporary” and are eventually destroyed in accordance with the Records Schedule.

Based on the RNL representative’s description of the deleted database, we determined Chapter 16 of the Records Schedule, Public Programs and Exhibitions, specifically File No. 1610-1, records relating to the planning and preparation of exhibits, including photographs, correspondence, and lists of exhibit items, could be applicable to the database.

According to the Records Schedule, these files should be identified as permanent and transferred to NARA in 5-year blocks when 10 years old. We made additional inquires with the RNL representative on whether there was another version of the record, electronic or paper, that included all of the information the deleted database contained. The representative responded the deleted database, created in RNL, was at most a reference or working copy, and the original, permanent record would have been created by the Exhibits Staff in Washington, DC.

NARA has a training, titled *Federal Records: What You Need to Know*, which all NARA employees are required to take on an annual basis through NARA’s Learning Management System (LMS). Our review of the training slides found it included general guidance for agency employees on the management of federal records and protection of federal records from unauthorized removal. However, the training did not include information on employees’ responsibility to cooperate with OIG, in accordance with NARA Directive 1201 and applicable laws and regulations, when records are requested during the performance of an audit.

The database did not contain any PII or otherwise sensitive information and had not been used for at least eight years, according to the RNL representative. The deletion was not escalated to an investigation.

## Recommendations

We recommend the Chief Operating Officer, in collaboration with the OIG:

> **Recommendation 9:** Issue an annual reminder to NARA staff of their responsibilities to cooperate with OIG audit requests, in accordance with NARA Directive 1201, the IG Act, as amended, and Title 18 U.S.C., Chapter 73, Section 1516, *Obstruction of Federal Audit*.

Management Response

NARA concurs with this recommendation. In collaboration with the OIG, the Chief Operating Officer will issue an annual reminder to NARA staff of their responsibilities to cooperate with OIG audit requests.

*Target Completion Date*: December 31, 2016

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

# Appendix A – MS Access Applications and Database Survey

Following is the result of the agency-wide MS Access Applications/ Databases survey NARA OIG conducted between August and October 2015, summarized into two tables. After a total of 740 applications/databases were initially identified from this survey, 1,060 additional applications/databases were reported, mostly from four Presidential Libraries.[12] Detailed survey responses for these additional applications/databases were not collected because the representatives stated they were outdated files that do not require conversion. Therefore, the tables only include survey results for the 740 applications/databases initially identified. Table A includes the count of applications/databases by Yes/No response to the survey questions; whereas Table B includes the count of applications/databases by NARA organization.

**Table A: Application/Database Count by Survey Question**

| Survey Question | Yes[13] | No |
|---|---|---|
| Currently in use? | 658 | 82 |
| ODBC connection setting | 38 | 660 |
| Username and password | 124 | 616 |
| Programming tools (e.g., Macro, VBA codes) | 251 | 460 |
| Does the database contain multimedia objects? | 15 | 725 |
| Does the database have a customer interface or application overlay (custom inputs and outputs) to access data? | 452 | 288 |
| Is this system data used to feed other critical strategic monitoring activities? | 164 | 576 |
| Does the database have a custom printout reports? | 337 | 401 |
| Is the database a public use finding aid? | 91 | 649 |
| Is the database accessed or shared by more than one site? | 72 | 668 |
| Is the database connected to any application or database? | 141 | 598 |
| Is the database a collector of metadata for records? | 263 | 477 |
| Is the database used as in input source for another system (such as ERA, HMS, DAS, etc.)? | 141 | 598 |
| Does the database need to be supported beyond the MS Access upgrade? | 491 | 210 |

[12] The additional applications/databases reported were from the following NARA organizations: Dwight D. Eisenhower Presidential Library (411); Richard Nixon Presidential Library (306); Lyndon B. Johnson Presidential Library (287); Jimmy Carter Presidential Library (54); and Office of the Inspector General (2).

[13] Although this table includes survey results for the 740 applications/databases, the sum of yes and no responses for each question may or may not equal to 740. This is due to the blank entries included in the responses for some applications/databases identified through the survey.

# Appendix A – MS Access Applications and Database Survey (Cont'd)

**Table B: Application/Database Count by NARA Organization**

| Org Code | Organization | Count |
|---|---|---|
| **AC** | Office of the Chief Records Officer | 12 |
| **AFC/AFO** | Federal Records Centers | 18 |
| **AFN** | National Personnel Records Center | 34 |
| **AISOO** | Information Security Oversight Office | 3 |
| **ANDC** | National Declassification Center | 11 |
| **B** | Business Support Services | 25 |
| **C** | Office of the Chief Operating Officer | 4 |
| **F** | Office of the Federal Register | 3 |
| **H** | Office of Human Capital | 1 |
| **I** | Office of Information Services | 5 |
| **LL** | Center for Legislative Archives | 17 |
| **LM** | Presidential Materials Division | 75 |
| **LP** | Office of Presidential Libraries (including the central office and 13 Presidential Libraries) | 442 |
| **NCON** | Congressional Affairs Staff | 1 |
| **NEEO** | Equal Employment Opportunity Office | 1 |
| **NGC** | General Counsel | 3 |
| **NHPRC** | National Historical Publications and Records Commission | 1 |
| **OIG** | Office of the Inspector General | 1 |
| **RDE** | Research Services Electronic Records Division | 7 |
| **S** | Office of Strategy and Communications | 74 |
| **V** | Office of Innovation | 2 |
| **Total** | | **740** |

# Appendix B – MS Access Database Scan

In August 2015, NARA's Information Security performed a scan of the machines attached to NARANet to detect machines with MS Access databases, using a tool named Triumfant. The scan detected MS Access databases from a total of 1,783 machines, and the report included information such as the machine name, date and time the database appeared, machine group (server and desktop types), and NARA site. Based on the information obtained from the scan, in conjunction with NARA's machine inventory report[14] and NARA employee listing as of August 2015[15], we matched the machine name to the respective NARA organization. We used the user's or the user's manager's name, whichever was available in the machine inventory report, to identify the respective NARA organization.

However, in many cases, the user or manager information for the machine only contained the NARANet user ID or nickname instead of the official first and last names of the user or manager as shown in the employee listing. In these cases, we used our best judgment to identify the user or manager's name, using the attributes such as the first initial and last name available from the user ID or nickname.

In addition, 534 of the 1,783 machines did not contain the user or manager information in the machine inventory report; therefore, we were unable to identify NARA organizations for these 534 machines. Further, 177 of the 1,783 machines were not included in the machine inventory report at all. As a result, NARA organizations for a total of 711 machines were not identified. We used the sites shown in the Triumfant scan report to count the number of machines for each NARA site.

As a result, we included the two summary tables, shown below, in this appendix. Table C reflects machine count by NARA organization, and Table D reflects machine count by NARA site.

[14] Provided by NITTSS.

[15] Provided by the Office of Human Capital (H).

# Appendix B – MS Access Database Scan (Cont'd)

**Table C: NARA Machine Count by Organization**

| Symbol | Organization | Machine Count |
|---|---|---|
| **A** | Agency Services | 360 |
| **B** | Business Support Services | 70 |
| **C** | Chief Operating Officer | 14 |
| **F** | Office of the Federal Register | 10 |
| **H** | Office of Human Capital | 55 |
| **I** | Office of Information Services | 75 |
| **L** | Legislative Archives, Presidential Libraries, and Museum Services | 188 |
| **N** | Office of the Archivist of the United States | 18 |
| **R** | Research Services | 240 |
| **S** | Office of Strategy and Communications | 18 |
| **V** | Office of Innovation | 24 |
| User information not available in machine inventory | | 534 |
| Machine not included in inventory | | 177 |
| | **Total** | **1783** |

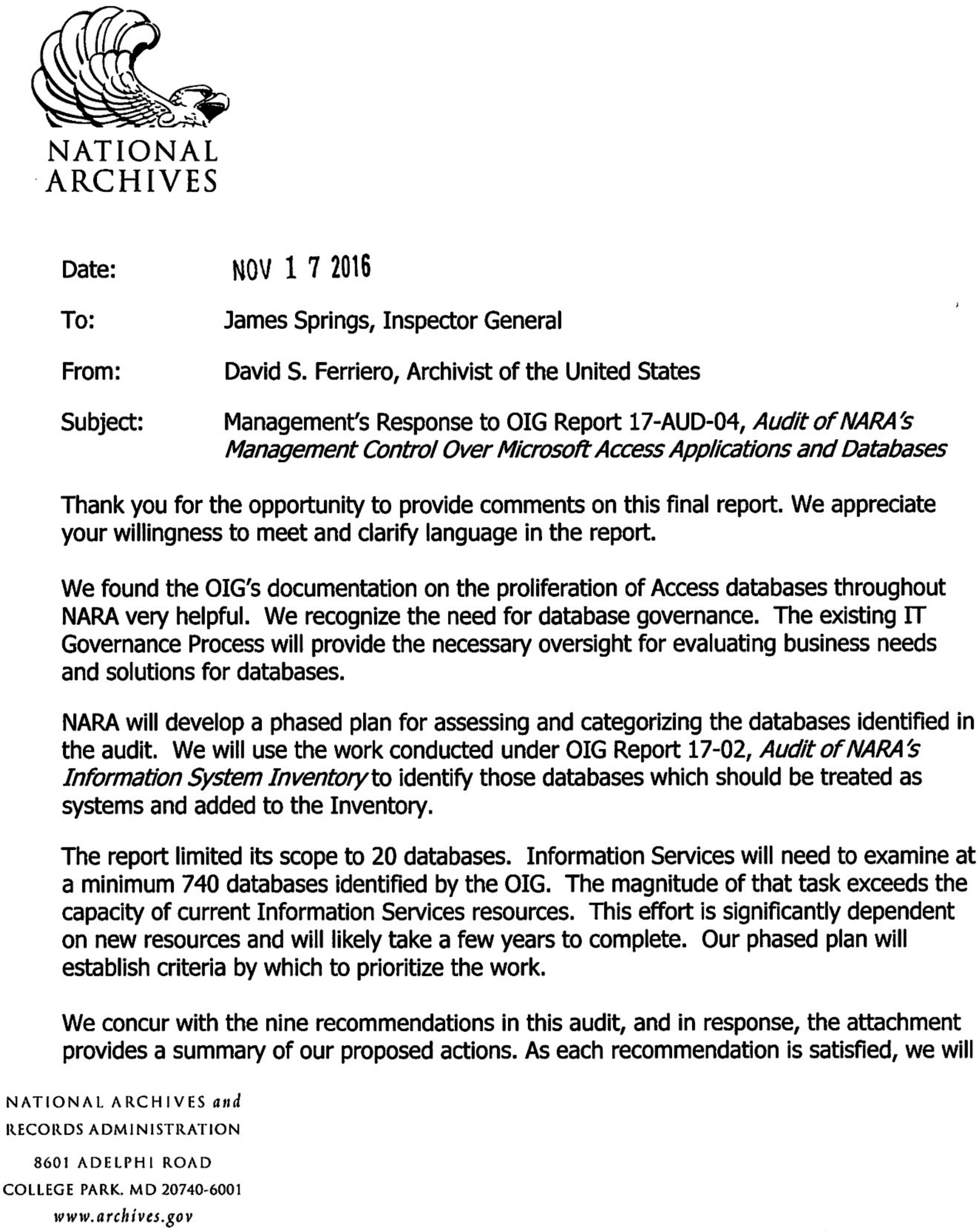
**Table D: NARA Machine Count by Site**

| Site | Machine Count |
|---|---|
| Archives I | 153 |
| Archives II | 586 |
| Broomfield | 18 |
| Jimmy Carter Library | 24 |
| Chicago | 16 |
| William J. Clinton Library | 17 |
| Dayton | 11 |
| Eisenhower Library | 17 |
| Ellenwood | 21 |
| Federal Register | 15 |
| Ford Library | 11 |
| Ford Museum | 8 |
| Fort Worth | 24 |
| George H. Bush Library | 14 |
| George W. Bush Library | 23 |
| Herbert Hoover Library | 9 |
| John F. Kennedy Library | 21 |
| Johnson Library | 16 |
| Kansas City | 28 |
| Laguna Niguel | 2 |
| Lee's Summit | 6 |
| Lenexa | 10 |
| Morrow | 14 |
| New York | 16 |
| Richard Nixon Library | 12 |
| Philadelphia | 21 |
| Ronald Reagan Library | 15 |
| Riverside | 24 |
| Rocket Center | 15 |
| Franklin D. Roosevelt Library | 20 |
| San Bruno | 12 |
| Seattle | 19 |
| Spanish Lake | 449 |
| Suitland | 13 |
| Valmeyer | 70 |
| Waltham | 22 |
| Site Information Unavailable | 11 |
| **Total** | **1,783** |

# Appendix C – Acronyms

| | |
|---|---|
| ADRRES | Archival Declassification, Review and Redaction System |
| ATO | Authorization-to-Operate |
| ARCIS | Archives and Records Centers Information System |
| CATS | Control and Tracking System |
| CIO | Chief Information Officer |
| DB | Database |
| ERA | Electronic Records Archive |
| FISCAM | Federal Information System Controls Audit Manual |
| FOIA | Freedom of Information Act |
| FRC | Federal Records Centers |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| HMS | Holdings Management System |
| ICP | Internal Control Program |
| ID | Identification |
| LMS | Learning Management System |
| MDR | Mandatory Declassification Review |
| MS | Microsoft |
| NARA | National Archives and Records Administration |
| NIST SP | National Institute of Standards and Technology Special Publication |
| NITTSS | NARA Information Technology & Telecommunication Support Services |
| NPRC | National Personnel Records Center |
| NSI | National Security Information |
| ODBC | Open Database Connectivity |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| OMPF | Official Military Personnel File |
| RRS | Researcher Registration Service |
| PII | Personally Identifiable Information |
| PMRS | Performance Management and Reporting System |
| SOP | Standard Operating Procedures |
| SQL | Structured Query Language |
| SOW | Statement of Work |
| U.S.C. | United States Code |
| VBA | Visual Basic for Applications |

# Appendix D – Management Response



NATIONAL
ARCHIVES

Date: NOV 1 7 2016

To: James Springs, Inspector General

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

Subject: Management's Response to OIG Report 17-AUD-04, *Audit of NARA's Management Control Over Microsoft Access Applications and Databases*

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

We found the OIG's documentation on the proliferation of Access databases throughout NARA very helpful. We recognize the need for database governance. The existing IT Governance Process will provide the necessary oversight for evaluating business needs and solutions for databases.

NARA will develop a phased plan for assessing and categorizing the databases identified in the audit. We will use the work conducted under OIG Report 17-02, *Audit of NARA's Information System Inventory* to identify those databases which should be treated as systems and added to the Inventory.

The report limited its scope to 20 databases. Information Services will need to examine at a minimum 740 databases identified by the OIG. The magnitude of that task exceeds the capacity of current Information Services resources. This effort is significantly dependent on new resources and will likely take a few years to complete. Our phased plan will establish criteria by which to prioritize the work.

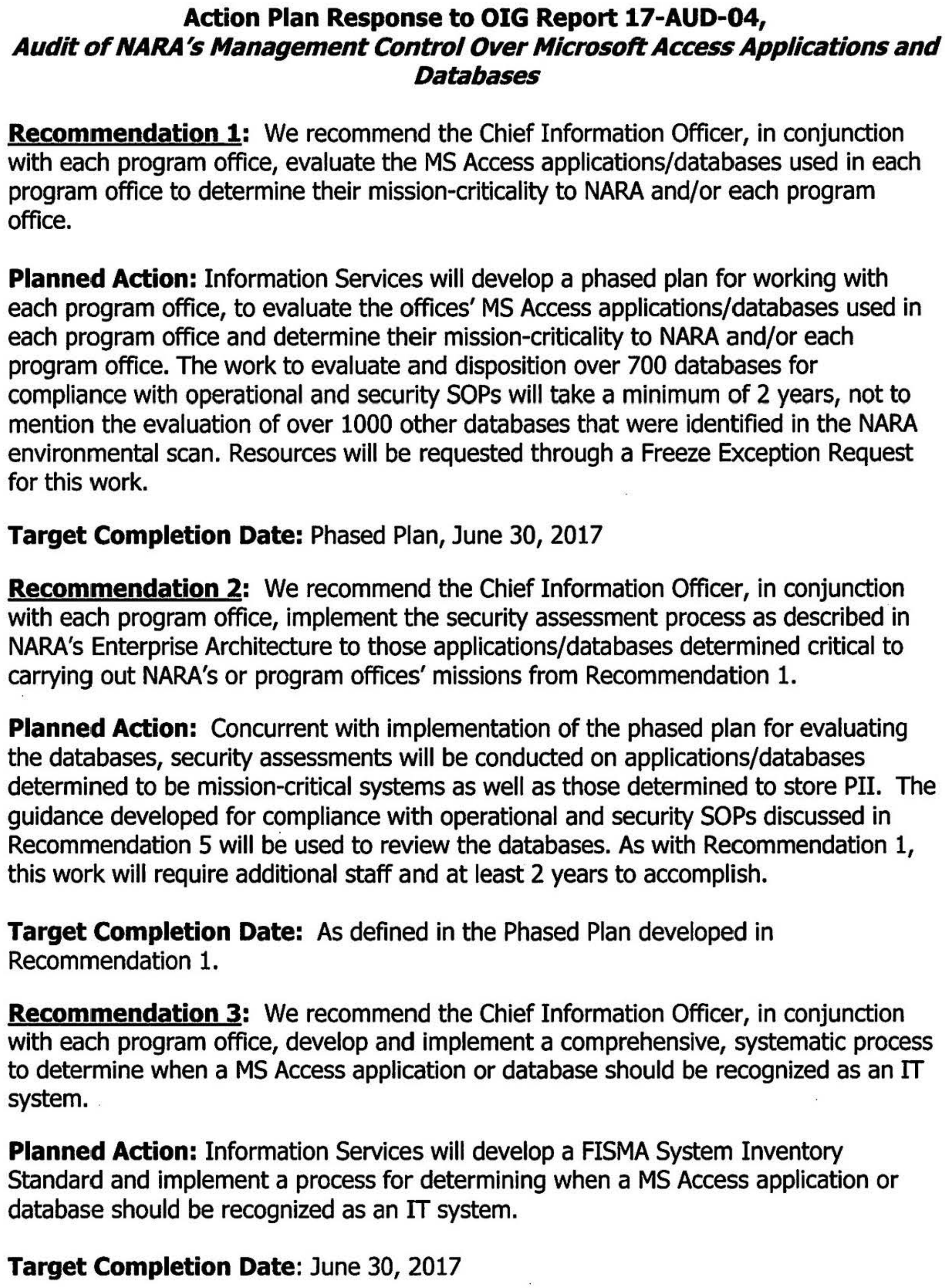
We concur with the nine recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will

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

provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Attachment



## Action Plan Response to OIG Report 17-AUD-04, *Audit of NARA's Management Control Over Microsoft Access Applications and Databases*

**Recommendation 1:** We recommend the Chief Information Officer, in conjunction with each program office, evaluate the MS Access applications/databases used in each program office to determine their mission-criticality to NARA and/or each program office.

**Planned Action:** Information Services will develop a phased plan for working with each program office, to evaluate the offices' MS Access applications/databases used in each program office and determine their mission-criticality to NARA and/or each program office. The work to evaluate and disposition over 700 databases for compliance with operational and security SOPs will take a minimum of 2 years, not to mention the evaluation of over 1000 other databases that were identified in the NARA environmental scan. Resources will be requested through a Freeze Exception Request for this work.

**Target Completion Date:** Phased Plan, June 30, 2017

**Recommendation 2:** We recommend the Chief Information Officer, in conjunction with each program office, implement the security assessment process as described in NARA's Enterprise Architecture to those applications/databases determined critical to carrying out NARA's or program offices' missions from Recommendation 1.

**Planned Action:** Concurrent with implementation of the phased plan for evaluating the databases, security assessments will be conducted on applications/databases determined to be mission-critical systems as well as those determined to store PII. The guidance developed for compliance with operational and security SOPs discussed in Recommendation 5 will be used to review the databases. As with Recommendation 1, this work will require additional staff and at least 2 years to accomplish.

**Target Completion Date:** As defined in the Phased Plan developed in Recommendation 1.

**Recommendation 3:** We recommend the Chief Information Officer, in conjunction with each program office, develop and implement a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system.

**Planned Action:** Information Services will develop a FISMA System Inventory Standard and implement a process for determining when a MS Access application or database should be recognized as an IT system.

**Target Completion Date:** June 30, 2017

**Recommendation 4:** We recommend the Chief Information Officer, in conjunction with each program office, determine all MS Access databases containing PII and ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.

**Planned Action:** MS Access databases containing PII will be among the first to be examined in the Phased Plan developed for Recommendation 1 to ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.

**Target Completion Date:** The phased plan delivered in Recommendation 1 will provide the target date for completing the analysis of MS Access databases containing PII. Information Services estimates the analysis will be finished by December 31, 2017.

**Recommendation 5:** We recommend the Chief Information Officer, in conjunction with each program office, develop and implement a process for future MS Access applications/databases created by program offices, including notification to and approval from the Office of Information Services for those that are mission-critical and/or contain PII or otherwise sensitive information.

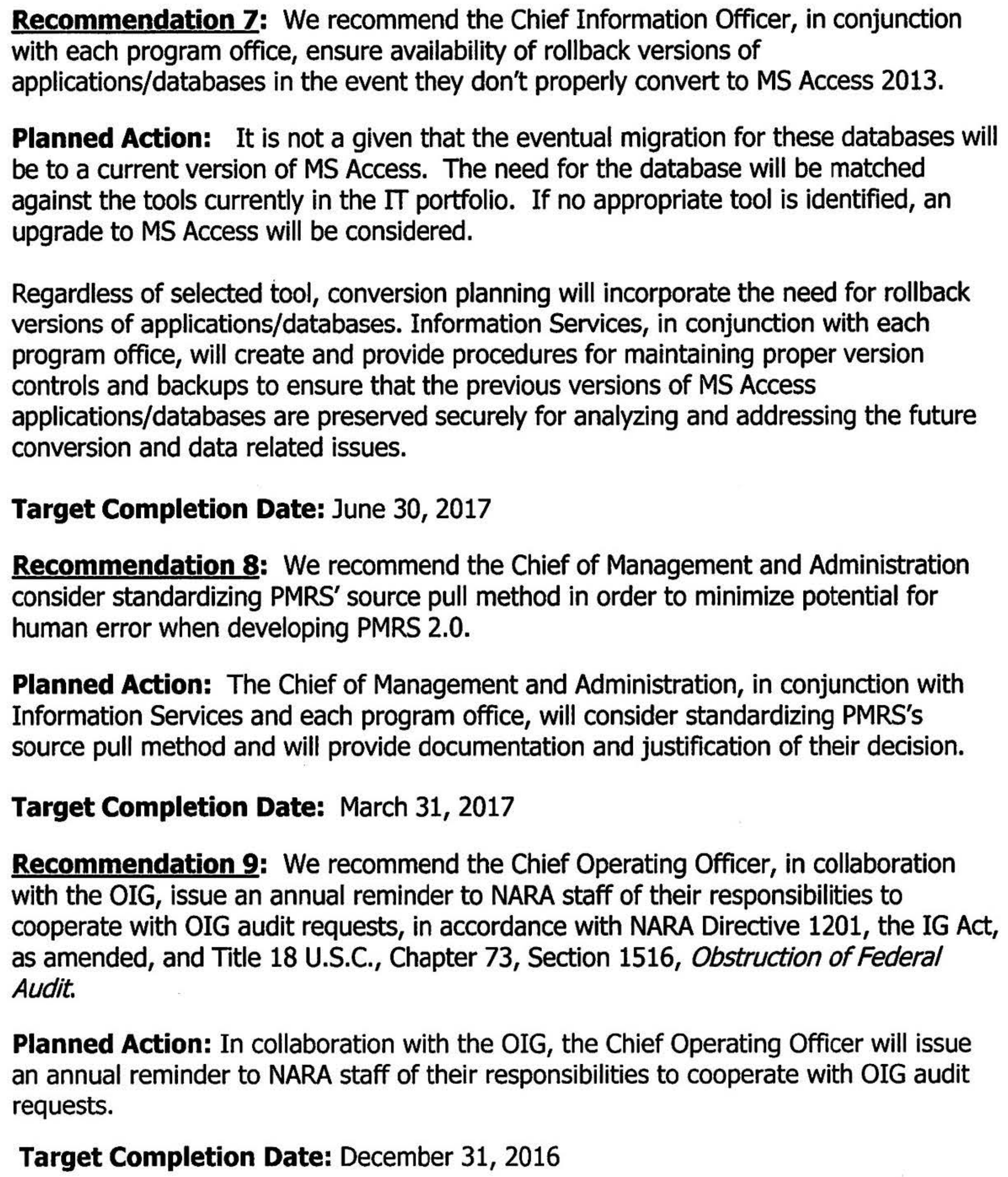
**Planned Action**: Information Services will incorporate database requirements within the IT governance process and directive. When an office identifies a database requirement, it will first develop a business need statement as defined in the IT governance process. That process will determine a solution that is sustainable by the OCIO.

**Target Completion Date:** April 30, 2017

**Recommendation 6:** We recommend the Chief Information Officer, in conjunction with each program office, identify all MS Access applications/databases containing programming languages and/or are source data for PMRS.

**Planned Action:** The phased plan developed in Recommendation 1 will include a review process for those applications/data bases containing programming languages and/or are source data for PMRS. Information Services, in conjunction with each program office, will evaluate the MS Access applications/databases used in each program office to evaluate and list the programming languages used for all the MS access applications/databases and create a list of current sources that feed data into PMRS.

**Target Completion Date:** June 30, 2017



**Recommendation 7:** We recommend the Chief Information Officer, in conjunction with each program office, ensure availability of rollback versions of applications/databases in the event they don't properly convert to MS Access 2013.

**Planned Action:** It is not a given that the eventual migration for these databases will be to a current version of MS Access. The need for the database will be matched against the tools currently in the IT portfolio. If no appropriate tool is identified, an upgrade to MS Access will be considered.

Regardless of selected tool, conversion planning will incorporate the need for rollback versions of applications/databases. Information Services, in conjunction with each program office, will create and provide procedures for maintaining proper version controls and backups to ensure that the previous versions of MS Access applications/databases are preserved securely for analyzing and addressing the future conversion and data related issues.

**Target Completion Date:** June 30, 2017

**Recommendation 8:** We recommend the Chief of Management and Administration consider standardizing PMRS' source pull method in order to minimize potential for human error when developing PMRS 2.0.

**Planned Action:** The Chief of Management and Administration, in conjunction with Information Services and each program office, will consider standardizing PMRS's source pull method and will provide documentation and justification of their decision.

**Target Completion Date:** March 31, 2017

**Recommendation 9:** We recommend the Chief Operating Officer, in collaboration with the OIG, issue an annual reminder to NARA staff of their responsibilities to cooperate with OIG audit requests, in accordance with NARA Directive 1201, the IG Act, as amended, and Title 18 U.S.C., Chapter 73, Section 1516, *Obstruction of Federal Audit*.

**Planned Action:** In collaboration with the OIG, the Chief Operating Officer will issue an annual reminder to NARA staff of their responsibilities to cooperate with OIG audit requests.

**Target Completion Date:** December 31, 2016

# Appendix E – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Deputy Chief Operating Officer
Chief of Management and Administration
Chief Information Officer
Deputy Chief Information Officer
Accountability

# OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically: https://www.archives.gov/oig/referral-form/index.html

Telephone: 301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail: IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821