OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001
www.archives.gov/oig

March 3, 2016

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs
Inspector General

SUBJECT: *Inadequate Information and Physical Security Controls at Select Federal Records Centers*

Attached for your action is our final report, *Inadequate Information and Physical Security Controls at Select Federal Records Centers*. We incorporated the formal comments provided by your office. The report contains eight recommendations aimed at improving controls over the security of electronic tracking and inventory systems and records in the custody of the National Archives and Records Administration's Federal Records Centers. Your office concurred with the eight recommendations.

In accordance with NARA Directive 1201, *Audits of NARA Programs and Operations*, section S7.m, within 45 days of the date of this memorandum, please provide our office with a written response that includes your (1) corrective action plan and (2) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

As with all OIG products, we will determine what information is publically 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 you 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.

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

OFFICE *of* INSPECTOR GENERAL

Inadequate Information and Physical Security Controls at Select Federal Records Centers

MARCH 3, 2016

OIG Audit Report No. 16-03

Table of Contents

Executive Summary

The Office of Inspector General's (OIG) audit of the National Archives and Records Administration's (NARA) Refile Processes in Federal Records Centers (FRCs) assessed the effectiveness and adequacy of management controls in place for the refile processes at selected FRCs. As a result of critical security issues discovered during the course of the audit, we expanded the objectives to assess the effectiveness of management controls related to information and physical security at Lee's Summit and Lenexa FRCs.[1] NARA's FRCs store records for agencies, including Official Personnel Folders (OPFs) for employees of the Internal Revenue Service (IRS) and select component agencies of the Department of Homeland Security (DHS).[2]

Lee's Summit maintains electronic tracking and inventory systems[3] to track the location of IRS and DHS OPFs. The systems maintain IRS and DHS employees' Personally identifiable information (PII), including names, social security numbers, and dates of birth. Information security controls for these systems were not adequate to protect PII, including access controls, protection of backup tapes and servers, and controls over data extracts. Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. Further, recent cyber-security incidents compromising current and former federal employees' PII highlighted the significance of ensuring proper safeguards are implemented to prevent similar attacks.

Lenexa stores permanent special media records in an 80,000 cubic foot cold storage facility and maintains a tracking database for the special media records' file location. Although additional holdings and physical security controls were implemented at some NARA offices after the theft of many special media records by a former employee,[4] weaknesses still exist. Lenexa's cold storage facility, which was separated from the main facility, had insufficient controls in place to safeguard special media records held in the cold storage facility. Weaknesses identified included the lack of monitoring of entry and exit activity, an updated key log, and a door to properly secure the facility. Further, proper information security controls were not in place to safeguard the special media records' file location. Agency Services management initiated immediate discussions

[1] This audit report represents one of two audit reports that will be issued. This report focuses on the information and physical security findings noted during the audit. The second report will discuss findings related to the refile processes at the FRCs.
[2] U.S. Customs & Border Protection, U.S. Citizenship & Immigration Services, and U.S. Immigration & Customs Enforcement.
[3] TAB FusionRMS designed the system maintained on sequel servers.
[4] The former employee was sentenced in 2012 for stealing sound recordings from NARA during his employment.

with Information Security management after the OIG identified the information security weaknesses.

This report contains eight recommendations to help strengthen controls over the security of electronic tracking and inventory systems and records in the custody of NARA's FRCs.

Background

National Archives and Records Administration's (NARA) Federal Records Centers Program (FRCP) Operations located within Agency Services: (1) receives records from Federal agencies for records center storage, servicing, or processing, pending their accession into NARA or other authorized disposition; and (2) services records by furnishing the records, or information from them, or copies of them, to Federal agencies and the public.

The Lee's Summit (AFOW-LS) Federal Records Center (FRC) serves agencies in New York, New Jersey, Puerto Rico, and the U.S. Virgin Islands. The Internal Revenue Service (IRS) and Department of Homeland Security (DHS) consolidated all of the Official Personnel Folders (OPFs) for employees they service into one location, at AFOW-LS in Missouri. As a part of the interagency agreements between NARA and these two agencies, NARA:

(1) provides all personnel and supervision necessary to manage, maintain, track, retrieve, and ship OPFs to authorized IRS and DHS representatives, other Federal agencies, and other authorized third parties;
(2) adheres to established privacy and security standards for "build out" of the physical site, established electronic databases, general data (computers, Automatic Data Processing (ADP)/telecommunications, etc.), and records management; and
(3) maintains electronic tracking and inventory systems for all IRS and DHS OPFs. The electronic tracking and inventory systems include a database of authorized requestors and provides a variety of reports to address the location of OPFs (where OPFs are located, who has OPFs charged out, when OPFs are due back, when OPFs are received back into the inventory, etc.).

The electronic tracking and inventory systems contain employee names, social security numbers, dates of birth, and the office where the employee works for each OPF held at AFOW-LS.

The Lenexa Federal Records Center (AFOW-LX) serves Federal agencies in Iowa, Kansas, Missouri, and Nebraska plus the Ogden IRS service center. AFOW-LX maintains an 80,000 cubic foot cold storage facility with two temperature controlled storage rooms that hold acetate based and color film, aerial film, overlays, motion pictures for Archives II and five presidential libraries, and microfilm of the 1960 and 2000 Censuses.

Objectives, Scope, Methodology

The audit objective was to assess the effectiveness and adequacy of management controls in place for (1) the refile processes and (2) information and physical security at Federal Records Centers (FRCs) located in Lee's Summit, Missouri and Lenexa, Kansas.

To accomplish our objectives, we interviewed representatives from AFOW-LX and AFOW-LS. We reviewed the interagency agreements between NARA and the IRS and DHS. We examined applicable Federal requirements and NARA guidance, including:

a. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
b. Privacy Act of 1974;
c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*;
d. NIST SP 800-123, *Guide to General Sever Security*;
e. Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*;
f. OMB Circular A-123, *Management's Responsibility for Internal Control*;
g. NARA *Information Technology* (*IT) Security Requirements* (Version 6);
h. NARA Directive 271, *Key Control at NARA Facilities;* and
i. NARA Directive 804, *IT Systems Security*;
j. NARA Directive 1571, *Archival Storage Standards*;
k. NARA Directive 1572, *Preventing Theft and Vandalism of NARA Holdings in NARA Facilities*.

This performance audit was conducted in accordance with generally accepted government auditing standards between June 2015 and January 2016. These 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 objective.

This audit was conducted by Kimberly Boykin, Senior Program Auditor, and William Brown, Program Auditor.

Audit Results

1. Insufficient information security controls for electronic tracking and inventory systems at Lee's Summit FRC.

Information security controls for the electronic tracking and inventory systems were not adequate to protect Personally identifiable information (PII), and prevent and detect unauthorized access. Specifically, weaknesses exist in access controls, the protection of servers and backup tapes, and controls over data extracts for the systems used to maintain and track IRS and DHS OPFs held at AFOW-LS. These weaknesses exist because management did not implement effective controls. Failure to provide adequate protections increases the risk of inappropriate disclosure of PII and unrestricted access to the systems.

According to the Privacy Act of 1974, each agency that maintains a system of records shall establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, outlines the minimum security requirement for Access Control; organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. Further, organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.[5] In addition, the interagency agreements between NARA and the IRS and DHS require NARA to adhere to established privacy and security standards for the establishment of electronic databases and general data (computers, ADP/telecommunications).

Servers and shared computers

The electronic tracking and inventory systems for the IRS and DHS OPFs are maintained on two non-network shared computers for AFOW-LS employees. DHS employees do not have access to the system for their records. However, IRS maintains office space

[5] Revised in 2013 and re-titled, *Security and Privacy Controls for Federal Information Systems and Organizations.*

next to AFOW-LS (separated from the records held at AFOW-LS) where IRS employees have computers in their office space allowing them to access the system for their OPF records. We noted the servers for the systems and the two computers used by the AFOW-LS employees were not secured and maintained in an area accessible by all of the AFOW-LS employees. NIST SP 800-123, *Guide to General Server Security*, indicates security should be considered from the initial planning stages of a server, including the physical security of the servers. It is critical that servers be located in secure physical environments, since many host sensitive information and should be treated as sensitive because of the damage to the organization's reputation that could occur if the servers' integrity is compromised.

Additionally, since the computers used by AFOW-LS employees were not connected to NARA's internal network (NARANet), the servers and computers were not serviced under NARA's IT contract. The AFOW-LS official was unable to tell us if the computers used by the IRS employees were setup like the computers used by the AFOW-LS employees. The official stated when NARA's new IT service contract was awarded in 2014, the Field Office System Administrator (FOSA) stopped servicing the computers because they were not a part of NARANet. When repairs or updates to the system were needed, an outside consultant was contracted by AFOW-LS.[6] Failure to properly secure the servers and computers allows the opportunity for unauthorized access to PII.

User accounts and passwords

A username and password was needed to log into the electronic tracking and inventory systems, however, during our visit the last employee signed into the IRS' system did not log off, which left the system vulnerable to unauthorized use. NIST SP 800-53 requires information systems to uniquely identify and authenticate users.

Our review of the IRS' system user list identified generic user accounts and user accounts no longer needed. Of the thirteen user accounts setup in the system, we noted:

- five user accounts were for employees that no longer worked at AFOW-LS or with the IRS OPFs;
- four user accounts were for current employees;
- three user accounts were generic (Administrator, Manager, and Editor); and
- one user account was shared by the IRS employees.

We could not determine how many user accounts had administrator rights, but we noted one employee was able to perform many of the same functions as a supervisor. NARA *Information Technology* (*IT) Security Requirements (Version 6)* (*IT Security*

[6] These contractors were required to sign a non-disclosure document when this work was performed.

Requirements) indicates for data requiring moderate or high confidentiality, NARA system owners shall employ the concept of least privilege and only allow access necessary to accomplish assigned tasks in accordance with organizational mission and business functions. For all data, NARA system owners shall review accounts' compliance with account management requirements at least annually. If user accounts no longer in use are not removed promptly, information in the system is at a greater risk of unauthorized disclosure.

Proper password requirements were not in place to protect the confidentiality of passwords and prevent unauthorized access. AFOW-LS employees with access to the systems indicated they did not follow the same password restrictions as their NARANet accounts and were not required to change the passwords on a periodic basis. The system password could be any password the user wanted and AFOW-LS personnel were not aware of NARA's password requirements. The on-site IRS employees shared the same user account and password to access the system. *IT Security Requirements* requires for all data, the information system, shall, for password-based authentication 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]. NARA Directive 804, *IT Systems Security*, indicates systems users are responsible for ensuring passwords and other access credentials are not shared or made available to unauthorized persons.

Backup and recovery

Written backup and recovery procedures (roles and responsibilities, the frequency and type of backups, and where the backups will be stored) did not exist for the electronic tracking and inventory systems. While AFOW-LS backs up the data maintained on the systems, the process to backup the data was not always followed nor was the backup data properly secured. The process for backing up the systems directed AFOW-LS staff to backup the system daily. However, the process was not always followed. As a result of our site visit, AFOW-LS began to backup the system daily onto Universal Serial Bus (USB) drives, which the FOSA rotates out once a week. The USB drives are kept in a lock box; however, the lock box is maintained in an unlocked drawer in an unlocked office. Additionally, the AFOW-LS official was not sure if the backup tapes were encrypted. *IT Security Requirements* requires the NARA system owner conduct backups of user-level and system-level information contained in the information system and to protect the confidentiality, integrity, and availability of backup information at the storage location. For data requiring high availability, the NARA information system administrator shall: (1) store backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational system; and (2) transfer information system backup information to the alternate storage site weekly. NARA Directive 1608, *Protection of*

Personally Identifiable Information (PII), requires NARA users to encrypt PII contained on portable devices, including external hard drives, laptops, USB flash drives, Personal Digital Assistants (PDAs), and other removable devices. Without information system backup controls to protect data backups, there is an increased risk recovery operations could be delayed or information could be lost.

Data extracts and monitoring activity

AFOW-LS employees were not restricted from performing data extracts of the electronic tracking and inventory systems, which contain sensitive PII. There was also no monitoring in place of user or administrator actions, such as audit logs, for unusual or inappropriate activity. A computer-readable data extract involves retrieving data from a database through a query and saving the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, states agencies must log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required. When we inquired if data extracts could be saved to a portable device, such as USB thumb drives, a user of the systems indicated it was allowed. Without controls in place over data extracts, sensitive PII is at an increased risk of disclosure. Additionally, failure to monitor user activity makes it difficult to investigate suspicious activity or suspected violations.

Agency Services management initiated immediate discussions with Information Security management after the OIG identified the information security weaknesses.

Recommendations

We recommend the Executive for Agency Services coordinate with the Chief Information Officer to:

Recommendation 1: Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and federal guidelines, including, but not limited to:

a. Determining the appropriate location of the system servers.
b. Determining if the servers and systems have the appropriate security protocols in place, including NARA standard software.
c. Reviewing user lists and determining the appropriate access for each account and eliminate any accounts no longer needed.
d. Implementing NARA password requirements.
e. Limiting users' ability to perform data extracts and ability to use portable devices.
f. Determining how to properly backup the systems and store the backup tapes.

g. Determining how to properly monitor user activity, including audit logs.
h. Ensuring all users have individual user accounts and passwords and do not share this information.

Recommendation 2: Establish a process for the Field Office System Administrator to service standalone databases maintained at FRCs, including the IRS and DHS electronic inventory systems.

Recommendation 3: Document procedures for the security of the IRS and DHS electronic tracking and inventory systems, including, but not limited to, access, backup and recovery, data extracts, and audit logs.

Recommendation 4: Ensure control procedures under NARA Directive 1608, *Protection of Personally Identifiable Information (PII),* are followed.

Management Response

Management concurred with the recommendations. Management stated they have assessed the electronic tracking and inventory systems identified in the report and will take appropriate actions to properly secure the data they contain. Management also highlighted in their response that the OIG report did not specifically identify the IRS and DHS electronic tracking and inventory systems as major information systems. Management does not consider the systems to be reportable in the agency's annual Federal Information Security Modernization Act (FISMA) report.

OIG Analysis of Management's Response

We agree the report does not specifically identify the electronic and inventory systems identified as major (FISMA-reportable information systems), however more stringent physical/logical security controls should be applied due to the type of information (PII) stored on the system.

2. Inadequate Physical and Information Security Controls for Lenexa FRC's Cold Storage Facility.

NARA did not have sufficient physical security controls in place to safeguard special media records stored in the cold storage facility (also referred to as the Ice Cube) at AFOW-LX. Additionally, the electronic tracking and inventory system used to track the records in the cold storage facility did not have proper information security controls in place. These weaknesses occurred because management did not implement management controls to properly safeguard records. OMB Circular A-123, *Management's Responsibility for Internal Control*, requires agencies to establish controls that reasonably ensure records are safeguarded against waste, loss, unauthorized use or misappropriation. NARA Directive 1571, *Archival Storage Standards*, indicates archival facilities must:

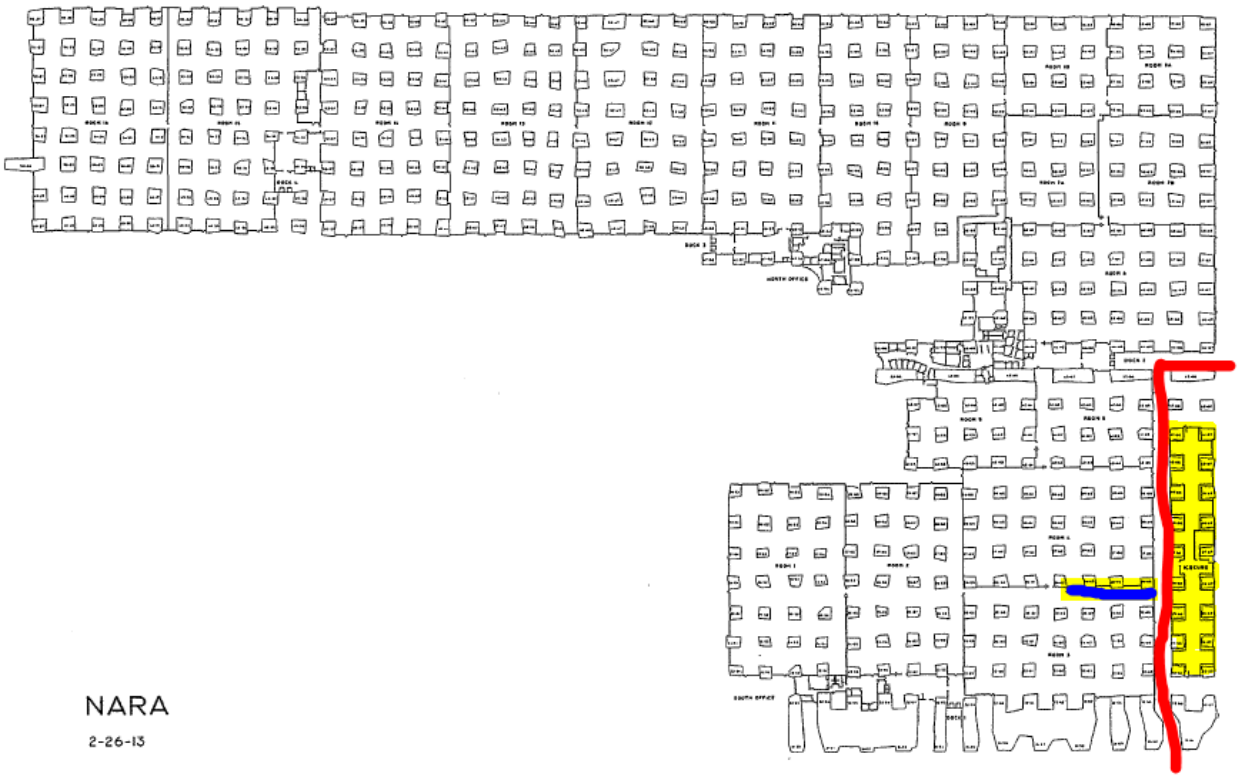
(1) comply, at a minimum, with the security specifications for a Level III facility as defined in the Department of Justice, U. S. Marshals Service report Vulnerability Assessment of Federal Facilities dated June 28, 1995;
(2) have an anti-intrusion alarm system to protect against unauthorized entry; and
(3) enforce controls on access to records storage areas.

Without sufficient physical security and information security controls in place, NARA is at risk of loss or theft of the permanent special media records stored in the cold storage facility at AFOW-LX.

Physical Security Controls

The AFOW-LX cold storage facility (see Exhibit No. 1 for a diagram of the facility layout) is separated from the main AFOW-LX facility with its own access door. AFOW-LX employees access the cold storage facility from Lenexa Executive Park's[7] access road (see Exhibit No. 2 for a picture of the access road) which is also accessible from an AFOW-LX exit door.

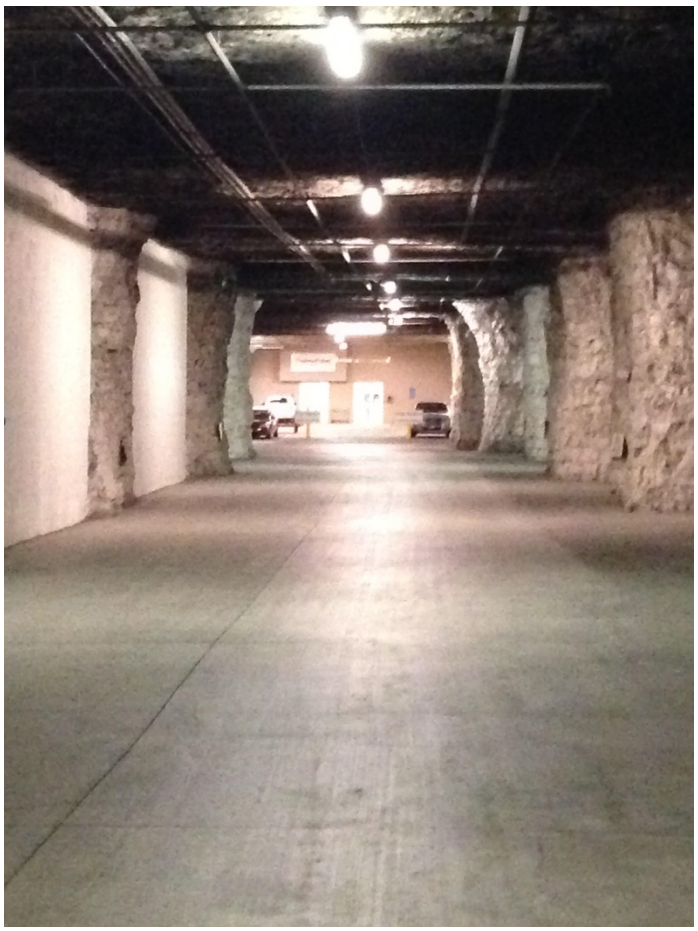
Exhibit No. 1 – AFOW-LX Facility Layout



[7] NARA leases space for AFOW-LX in an underground business complex operated by a third party vendor.

* The yellow highlighted area on the bottom right is the cold storage facility; the red line is the access road; and the blue line is the walkway from the facility exit door to the access road.

Exhibit No. 2 – Access Road



Physical security controls for the cold storage facility had not been properly implemented. There were no exterior or interior cameras or recording monitors to observe activity for the cold storage facility. The road to the facility is also accessible to other tenants of Lenexa Executive Park, but there was no ability to monitor entry and exit activity and other activity outside the door of the cold storage facility. There is an intrusion detection system on the cold storage facility's door connected to the AFOW-LX system and alarmed after hours. However, authorized employees or visitors entering and exiting the cold storage facility were not monitored or required to sign in and out of the cold storage facility. AFOW-LX's official indicated budget constraints have prevented the facility from installing additional cameras throughout the facility.

The door to the cold storage facility did not appear adequate to protect the records stored there. The door is the only entrance point for the cold storage facility and is a keyed solid

metal entry door (see Exhibit No. 3). However, during our visit, we observed an attempt by an AFOW-LX official to open the locked door resulted in the door slightly budging.

Further, an updated Key Control Log was not maintained. When the OIG requested the log, AFOW-LX's official updated it during our visit because there were several employees listed no longer working at the facility. NARA Directive 271, *Key Control at NARA Facilities*[8], indicates the primary key custodian is responsible for securing, inventorying, issuing, and receiving returned keys. Additionally, the directive indicates retained stock key changes of inventory during initial acquisition, loss, issue, return, key reproduction, or system expansion must be documented by the primary key custodian on the Key and Blank Inventory Register. Issued keys reflected on this Register must agree with keys issued on the Key Control Log.

Exhibit No. 3 – Cold Storage Facility Door

[8] NARA 271 was updated on October 19, 2015 after our fieldwork was completed.

Without security cameras in place to monitor access, employees could exit the cold storage facility with valuable special media records and not be observed. If NARA found records were missing, it would be unable to view security footage to identify when the records may have been removed. NARA also would not have evidence of which employees entered the facility on any particular day.

BX Physical Security Inspections

NARA's Security Management Division (BX) completed a Facility Security Assessment and Inspection at AFOW-LX in August 2011. We reviewed the report from the inspection and it did not discuss the cold storage facility maintained at AFOW-LX. We inquired with a Field Support Officer about the security of the cold storage facility. The staff member indicated the risk of theft from the facility was high. The staff member also indicated the security specialist who performed the inspection did not review the security at the cold storage facility, which may have been due to time constraints. In response to the findings in the Facility Security Assessment and Inspection Report, a previous AFOW-LX official recommended more time be allowed for future inspections. NARA Directive 1572, Preventing Theft and Vandalism of *NARA Holdings in NARA Facilities*, indicates BX: (1) conducts inspections of secure areas of NARA-occupied facilities, or reviews contractor-prepared inspection reports, as part of the cycle of security and workplace inspections, and otherwise works with NARA custodial units to assure that facilities are suitable for securing NARA holdings until on-site, physical inspections can be conducted; and (2) advises NARA custodial units on appropriate measures to secure holdings in their area of responsibility, including advice for preparation of local directives implementing physical and personnel security.

Information security controls

AFOW-LX maintains an electronic tracking and inventory system[9] (separate from Archives and Records Centers Information System (ARCIS)[10]) in the cold storage facility. The system tracks the location of all special media records stored including the shelf location of the records and when those records are added or removed from the facility. It does not contain written descriptions (e.g. World War II video) of the records, but descriptive file numbers (e.g. ABC123).

Information security controls for the system were not sufficient to prevent and detect unauthorized access. Specifically, we noted the system was located on the hard drive of the computer in the cold storage facility. Although, the system was recently connected to

[9] TAB FusionRMS designed the system.
[10] The web-based system is the online portal through which agencies can do business with the FRCs. ARCIS allows agencies to conduct all transactions online, saving them time and reducing paperwork. The system also lets agencies track transactions electronically, giving them instant access to information about their records.

NARANet, during our visit it was still located on the hard drive. Backups were performed daily, but they were saved to a thumb drive. There was also an outdated backup located on Google Drive for Archives II and presidential libraries users to access. Failure to properly secure the system and its backup poses a threat to the location information for the 80,000 cubic feet of special media records stored in the facility.

Currently, several AFOW-LX employees have physical access to the cold storage facility. Although, their job responsibilities may not require them to access the system, there are no controls in place to prevent their access. The user ID and password for the system was taped to the computer and available for anyone to use as long as they could log into the computer. Without unique usernames and passwords for the system, NARA cannot track user activity in the database.

Recommendations

We recommend the Executive for Agency Services:

Recommendation 5: Coordinate with NARA's Security Management Division to implement enhanced physical security controls for the AFOW-LX cold storage facility, including, but not limited to:

a. Performing a security risk assessment to determine if the facility is properly secured.
b. Installing additional security measures to properly secure the records (e.g. door, locks, card reader, and cameras).
c. Implementing a log to properly monitor individuals entering and exiting the facility.

Recommendation 6: Ensure all Federal Records Centers are following key control procedures under NARA Directive 271, *Key Control at NARA Facilities.*

Recommendation 7: Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and federal guidelines, including, but not limited to:

a. Determining the appropriate location of the system server.
b. Determining if the server and system has the appropriate security protocols in place, including NARA standard software.
c. Reviewing user lists and determining the appropriate access for each account and eliminate any accounts no longer needed.
d. Implementing NARA password requirements.
e. Determining how to properly backup the system and store the backup tapes.
f. Determining how to properly monitor user activity, including audit logs.
g. Ensuring all users have individual user ids and passwords and do not share this information.

Recommendation 8: Provide only authorized users access to the cold storage system.

Management Response

Management concurred with the recommendations.

Appendix A – Acronyms

ADP	Automatic Data Processing
AFOW-LS	Lee's Summit Federal Records Center
AFOW-LX	Lenexa Federal Records Center
ARCIS	Archives and Records Centers Information System
BX	Security Management Division
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FOSA	Field Office System Administrator
FRC	Federal Records Center
FRCs	Federal Records Centers
FRCP	Federal Records Centers Program
IRS	Internal Revenue Service
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPF	Official Personnel Folders
PDA	Personal Digital Assistant
PII	Personally identifiable information
SP	Special Publication
USB	Universal Serial Bus

Appendix B – Management Response

NATIONAL ARCHIVES

Date: FEB 1 8 2016

To: James Springs, Inspector General

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

Subject: OIG Draft Audit Report 16-03, *Inadequate Information and Physical Security Controls at Select Federal Records Centers*

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 have assessed the electronic tracking and inventory systems identified in the report and will take appropriate actions to properly secure the data they contain. The report does not specifically identify them as major information systems and we do not consider them to be reportable in the agency's annual Federal Information Security Modernization Act report.

We concur with the eight 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

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Executive for Agency Services
Executive for Business Support Services
Chief Information Officer
Chief Information Security Officer
Audit Liaison

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