OFFICE *of* INSPECTOR GENERAL

SEMIANNUAL REPORT *to* CONGRESS

OCTOBER 1, 2015 *to* MARCH 31, 2016

NATIONAL ARCHIVES

FOREWORD

I am pleased to present this Semiannual Report to the Congress covering the oversight activities of the Office of Inspector General (OIG) for the National Archives and Records Administration (NARA) from October 1, 2015 to March 31, 2016. Our audits and investigations continue to assess the effectiveness, efficiency, economy, and integrity of NARA's programs and operations.

NARA's has the unique mission of identifying, storing, accessing, protecting, preserving and providing access to the permanently valuable records of all three branches of the Federal Government. NARA works with other agencies to help them manage their records from creation until they are either properly disposed of, or transferred to NARA. NARA also provides other agencies temporary record's storage on a fee-for-service basis. Once permanent records are transferred to NARA, the agency stores and preserves them so the public may access the records in perpetuity. NARA provides access through research rooms across the country, mail and email correspondence, private sector partners, on-line at archives.gov, and various social media outlets.

NARA faces many significant challenges and obstacles; the most significant are detailed in the "NARA Top Ten Challenges" section of this report. Our audits and investigations continue to point out the difficulty in addressing these challenges, now and in the future, due to the growing volume of records and technology advances. NARA needs to assess and modify how it does business, and transition its programs and operations to more economical and efficient models.

NARA must also continue to work to ensure Congress is fully aware of the challenges and constraints hindering the agency from accomplishing its mission. For example, the Archivist of the United States testified before the House Committee on Oversight and Government Reform's Subcommittee on Government Operations that "the ability for us to do more with less has been reached-we're at the point where we can't do more with less. We have not-the appropriate level of staffing to do the job that we need to do."

My office stands ready to assist the agency. The OIG can and will be a constructive force, helping the agency accomplish its mission in this time of great challenge. Through the application of our independence, expertise, and due diligence we will strive to serve as a significant asset to our many customers.

Finally, I am honored to welcome Jewel Butler as the new Assistant Inspector General for Audits. Jewel is already hard at work contributing to the office, and making our audit program better. I continue to be proud of the hard work and dedication of my staff, and commend their efforts. I am also appreciative of management's efforts to assist the OIG in completion of our audit and investigative efforts.

James Springs

James Springs
Inspector General

TABLE OF CONTENTS

Visit http://www.archives.gov/oig/ *to learn more about the National Archives Office of Inspector General.*

EXECUTIVE SUMMARY

This is the 55th Semiannual Report to Congress summarizing the activities and accomplishments of the National Archives and Records Administration (NARA) Office of Inspector General (OIG). A summary of NARA's top ten management challenges is included as well. The highlights of our major functions are summarized below.

Audits and Reports

The Office of Audits continued to assess the economy and efficiency of NARA's programs and operations, and examine NARA's Information Technology (IT) systems including the Electronic Records Archives (ERA). During the reporting period, the Office of Audits issued the following audit reports.

Information Technology (IT)

- **NARA's Web Hosting Environment.** NARA did not provide consistent oversight and management of the agency's web hosting environments. NARA did not classify or categorize its internal web hosting environment in accordance with federal information security standards, and numerous control weaknesses exist within NARA's internal web hosting environment. As a result, NARA lacks assurance information security protections are in place commensurate with the risk to the confidentiality, integrity, and availability of NARA's internal web hosting environment. (OIG Audit Report #16-01, dated October 19, 2015. See page 12.)

- **NARA's Compliance with FISMA (for Fiscal Year 2015).** Although NARA generally had policies for its information security program, its implementation of those policies was not fully effective to preserve the confidentiality, integrity, and availability of the agency's information and information systems. This potentially exposed NARA to unauthorized access, use, disclosure, disruption, modification, or destruction. NARA indicated these weaknesses represent long-standing issues in its security environment. Further, NARA stated these issues were due to inadequate management resources and budget for many years; a lack of effectively implemented processes and procedures; and corrective actions requiring long term solutions. (OIG Audit Report #16-02, dated January 15, 2016. See page 13.)

- **NARA's Publicly Accessible Websites.** NARA does not provide adequate management and does not have strong internal controls in place to ensure the security of its publicly accessible websites. As a result, NARA has reduced assurance all of the websites the agency is responsible for —including those processing personally identifiable information (PII)—are secure, adequately protected, and/or compliant with Federal security standards. Additionally, NARA has not securely and consistently configured a secure protocol for data transfer (HTTPS) on its websites and lacks assurance they provide the strongest protection available. Finally, NARA has not reviewed security assessments for cloud web hosting providers, and the agency lacks assurance its cloud web hosting environments are adequately secure. (OIG Audit Report #16-05, dated March 25, 2016. See page 13.)

Programs and Operations

- **Inadequate Information and Physical Security Controls at Select Federal Records Centers.** NARA did not provide adequate information and physical security controls to protect PII, access controls, backup tapes and servers, and data extracts. NARA also lacked proper information security controls to safeguard the location where special media records were stored—increasing the risk of loss or theft of these important records. Other weaknesses included the lack of entry and exit monitoring, an updated key log, and a properly secured door to the facility. Without proper controls in place, 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. (OIG Audit Report #16-03, dated March 3, 2016. See page 14.)

- **NARA's Fiscal Year 2015 Financial Statements Independent Audit Report.** NARA received an unmodified opinion on its financial statements. There was one significant deficiency in internal controls over financial reporting related to information technology. There were no material weaknesses in internal controls over financial reporting and no instances of noncompliance with certain provisions of laws and regulations. (OIG Audit Report #16-04, dated December 21, 2015. See page 15.)

Investigations

The Office of Investigations (OI) receives and evaluates complaints and conducts investigations related to fraud, waste, and abuse in NARA programs and operations. This includes identifying and recovering wrongfully alienated NARA holdings. Investigations showing violations of law, regulations, rules, or contract terms may result in administrative, civil, or criminal actions. These can include terminations, debarments, prison terms, probation, fines, restitution, and other actions. The OI may also issue management letters detailing specific problems or vulnerabilities and offer insight on how to correct them.

In this period the OI opened 11 investigations, while closing four, including one criminal conviction. Prosecutors declined to accept three individuals referred for prosecution.

Other notable achievements include:

- Last period the OI began an agency-wide outreach program educating NARA employees at field sites across the nation regarding responsibilities of the OIG and NARA employees concerning waste, fraud, and abuse. We have received positive feedback from all of the NARA offices visited to date, and this program has resulted in additional allegations being reported. We plan to continue this program to assist NARA staff with understanding OIG and NARA responsibilities.
- In addition to our outreach briefings to the field, the OI also provides the same brief to all incoming NARA employees at NARA's facility in College Park, MD. This ensures many of NARA's new employees are introduced to the OIG and our mission as early as possible. Between the outreach briefings and the new employee orientation briefings, OI staff conducted nine briefings to 76 NARA employees.

Management Assistance and Other Work

In addition to audits and investigations, the OIG continued to assist NARA and others in various ways, including the following highlights from the period.

- Became aware that the SF-180 form for requesting veterans' records had been changed to eliminate the specific option for veterans to request their complete record. Check blocks for specific types of commonly requested documents were available, but the check block for requested the complete record was removed. Worked with management officials to publicize on the NARA website the process veterans could use to request their complete record.
- Worked with the agency at the end of the last reporting period to have the Archivist of the United States issue an agency-wide notice to all employees emphasizing their duty to report information to the OIG. After issuance the OI worked with several offices that came forward with information they did not realize they should be routinely sharing to coordinate new processes and ensure all potentially relevant information reaches the OIG.
- Continued running the Whistleblower Ombudsman program, providing training and information to potential whistleblowers on various rules and protections available. This work included one-on-one consultations with four individuals, and a meeting with the Senate Whistleblower Caucus.
- Responded or worked on 10 requests for OIG records under the Freedom of Information Act (FOIA), including requests for more than 24 Reports of Investigation and the review of a 244-page Report of Investigation.
- Reviewed aging administrative cases from the Archival Recovery Team for potential referral to NARA's new Archival Recovery Program for follow-up and monitoring.
- Provided comment and input into several NARA directives and regulations covering a variety of topics.
- Coordinated with agency general counsel to get OIG portion of a civil suit listing the Inspector General as a defendant handled concurrently by Assistant US Attorney.
- Worked with agency IT contractors and NARA employees working on OIG systems to ensure relevant individuals had signed confidentiality/non-disclosure agreements in place.
- Responded to 19 requests from NARA for reviews of proposed legislation, Office of Management and Budget (OMB) regulations, Congressional testimony, and other items.

INTRODUCTION

About the National Archives and Records Administration

Mission

The National Archives and Records Administration (NARA) drives openness, cultivates public participation, and strengthens our nation's democracy through public access to high-value government records. Simply put, NARA's mission is to preserve and provide public access to Federal Government records in its custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

Background

By preserving the nation's documentary history, NARA serves as a public trust on which our democracy depends. It ensures continuing access to essential evidence documenting the rights of American citizens, the actions of Federal officials, and the national experience. Through NARA, citizens can inspect for themselves the public record of what the government has done. Thus it enables agencies to review their actions, and it helps citizens hold them accountable.

Federal records reflect and document America's development over more than two centuries. They are great in number, diverse in character, and rich in information. NARA holds nearly 4.9 million cubic feet of traditional records. These holdings also include, among other things, letters, reports, architectural/engineering drawings, maps and charts; moving images and sound recordings; and photographic images. Additionally, NARA maintains nearly 647,000 artifacts and approximately 678 terabytes of electronic records. The number of records born and stored solely in the electronic world will only continue to grow; thus NARA developed the Electronic Records Archives to attempt to address this burgeoning issue.

NARA involves millions of people in its public programs, including exhibitions, tours, educational programs, film series, and genealogical workshops. In FY 2015, NARA had 61 million online visits in addition to hosting 3.5 million traditional museum visitors, all while responding to almost one million written requests from the public. NARA also publishes the *Federal Register* and other legal and reference documents, forming a vital link between the Federal Government and those affected by its regulations and actions. Through the National Historical Publications and Records Commission, NARA helps preserve and publish non-Federal historical documents that also constitute an important part of our national heritage. Additionally, NARA administers 13 Presidential libraries preserving the papers and other historical materials of all past Presidents since Herbert Hoover.

Resources

In Fiscal Year (FY) 2016, NARA was appropriated $389 million. This included $372.4 million for operating expenses, $7.5 million for repairs and restoration of NARA-owned buildings, $5 million for the National Historical Publications and Records Commission (NHPRC), and $4.18 million for IG operations. With approximately 2,833 full-time equivalents (FTEs), NARA operates 43 facilities nationwide.

INTRODUCTION

About the Office of Inspector General (OIG)

The OIG Mission

The OIG serves the American citizen by improving the effectiveness, efficiency, and economy of NARA programs and operations. As part of our mission, we detect and prevent fraud and abuse in NARA programs and strive to ensure proper stewardship over Federal funds. We accomplish this by providing high quality, objective audits and investigations and serving as an independent, internal advocate. Unique to our mission among other OIGs is our duty to ensure NARA protects and preserves the items belonging in our holdings, while safely providing the American people with the opportunity to discover, use, and learn from our documentary heritage.

Background

The Inspector General Act of 1978, as amended, along with the Inspector General Reform Act of 2008, establishes the OIG's independent role and general responsibilities. The Inspector General keeps both the Archivist of the United States and Congress fully and currently informed on our work. The OIG evaluates NARA's performance, makes recommendations for improvements, and follows up to ensure economical, efficient, and effective operations and compliance with laws, policies, and regulations. In particular, the OIG:

- assesses the effectiveness, efficiency, and economy of NARA programs and operations;
- recommends improvements in policies and procedures to enhance operations and correct deficiencies;
- recommends cost savings through greater efficiency and economy of operations, alternative use of resources, and collection actions; and
- investigates and recommends actions to correct and prevent fraud, waste, abuse, or mismanagement.

Further, the OIG investigates criminal and administrative matters concerning the agency, helping ensure the safety and viability of NARA's programs, customers, staff, and resources.

Resources

In FY 2016, Congress provided $4.18 million for the OIG, including authorization for 24 FTEs. During this period three positions were filled, the Assistant Inspector General for Audits (AIGA) and two criminal investigators. Currently the OIG has 17 FTEs on board, including an Inspector General, one support staff, seven FTEs devoted to audits, seven FTEs devoted to investigations, and a counsel to the Inspector General.

Involvement in the Inspector General Community

Council of Inspectors General on Integrity and Efficiency (CIGIE) Legislation Committee

The Legislation Committee provides timely information about congressional initiatives to the IG community; solicits the views and concerns of the community in response to legislative initiatives and congressional requests; and presents views and recommendations to congressional committees and staff, the Government Accountability Office, and the Office of Management and Budget on issues and legislation affecting the IG community. The OIG counsel attends Committee meetings for the IG, who serves as a member. During this period counsel was involved in various aspects of the Committee's work including assisting in creating a draft views letter on S.579, the Inspector General Empowerment Act; providing data for S.1378, the Bonuses for Cost Cutters Act; developing input for S.2450, the Administrative Leave Act; and proposed legislative changes to OIG reporting requirement on open audit recommendations and others.

CIGIE Audit Committee

The Audit Committee provides leadership to, and serves as a resource for, the Federal Inspector General audit community. Specifically, the Audit Committee sponsors and coordinates audit-related activities addressing multi-agency or Government-wide issues, maintains professional standards for OIG audit activities, and administers the audit peer review program. The Audit Committee also provides input to the CIGIE Professional Development Committee on training and development needs of the CIGIE audit community, and advice to the Chairperson, Vice Chairperson, and Executive Director regarding CIGIE's contracts for audit services. The AIGA attends Committee meetings for the Inspector General, who serves as a Committee member.

CIGIE Investigations Committee

The Investigations Committee advises the community on issues involving criminal investigations and investigative personnel. The Committee also works on establishing criminal investigative guidelines. The Assistant Inspector General for Investigations (AIGI) attends these meetings for the Inspector General, who is a member. The AIGI is involved in helping provide guidance, assistance, and support to the CIGIE Investigations Committee in the performance of its duties.

Council of Counsels to Inspectors General (CCIG)

The OIG counsel continues to be an active member of the CCIG. The CCIG provides a rich environment wherein legal issues can be raised and interpretations can be presented and reviewed with an experienced network of OIG lawyers.

CIGIE Training Institute

The OIG counsel continued to work with the CIGIE Training Institute teaching the Inspector General Authorities course.

Whistleblower Ombudsman Working Group (WOWG)

In accordance with the spirit of the Whistleblower Protection Enhancement Act of 2013, the OIG formed a whistleblower ombudsman program and is working with the WOWG to develop best practices and implement an effective training program.

Peer Review Information

Peer Review of NARA OIG's Audit Organization

The NARA OIG audit function was last peer reviewed by the Federal Deposit Insurance Corporation (FDIC) OIG in accordance with the Government Accountability Office's *Government Auditing Standards* (GAS) and CIGIE's *Guide for Conducting External Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*. FDIC OIG concluded:

"The system of quality control for the audit organization of the NARA OIG, in effect for the 12 months ended September 30, 2013, has been suitably designed and complied with to provide the NARA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Federal audit organizations can receive a rating of *pass; pass with deficiencies,* or *fail.* NARA OIG has received a peer review rating of *pass*."

The peer review report's accompanying letter of comment contained 14 recommendations that, while not affecting the overall opinion, were designed to further strengthen the system of quality control in the NARA OIG Office of Audits. We completed actions on all but two of the agreed upon recommendations and currently plan to have full implementation of the two outstanding recommendations by September 30, 2016.

Outstanding Recommendations: The FDIC OIG recommended that the Acting Inspector General revise the Procedures Manual to (1) require that auditors request a description of planned corrective actions to address recommendations from NARA management before finalizing audit reports and memoranda, and (2) include a process for addressing situations in which NARA management does not provide corrective action plans in its responses to audit reports and memoranda. The corrective actions necessary also involved changing NARA management's process, which they were not able to immediately implement. A process has been drafted, agreed upon by the agency, and is currently being piloted. Full implementation is anticipated by September 30, 2016. There are no other outstanding recommendations from any peer review of the NARA OIG that have not been fully implemented. The peer review report (the system review report) is posted on our website at *http://www.archives.gov/oig/reports/audit-reports-2012.html.*

NARA OIG Peer Review of the Securities and Exchange Commission OIG

NARA OIG completed a peer review of the audit operations of the Securities and Exchange Commission (SEC) OIG and issued a final report to them on December 29, 2015. In our opinion, the system of quality control for the audit organization of SEC OIG in effect for the year ended March 31, 2015, has been suitably designed and complied with to provide SEC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. SEC OIG received an External Peer Review rating of pass.

As is customary, we also issued a Letter of Comment setting forth findings and recommendations not considered significant enough to affect our opinion in the system review report. We made six recommendations and identified one matter for consideration. SEC OIG agreed with all six recommendations. SEC's planned actions adequately addressed the six recommendations.

Peer Review of NARA OIG's Office of Investigations

In January 2016, a team of Special Agents from the Treasury OIG conducted a comprehensive, multi-day, review of the Office of Investigations' operations in accordance with CIGIE's current "Quality Standards for Investigations." On February 1, 2016, Treasury's assessment team found our system of internal safeguards and management procedures for investigations to be in full compliance with all applicable guidelines and regulations. There are no outstanding recommendations from this review.

Response to Congressional Items

In addition to communicating and meeting with Congressional staff over the period to keep the Congress informed about agency and OIG activities, the OIG responded to the following items.

NARA's Space Management Challenge

NARA is running out of room to physically store permanent records. The IG met with staff members from various oversight committees to inform them of NARA's serious challenges in space management.

Ongoing Report Requested by Chairman Johnson and Chairman Grassley

The OIG responded to a letter signed by Senator Ron Johnson, Chairman of the Committee on Homeland Security and Governmental Affairs, and by Senator Charles Grassley, Chairman of the Committee on the Judiciary, requesting several items of information on a continuing basis. Among other things, our response included information on outstanding unimplemented audit recommendations, descriptions of products provided to the agency but not responded to within 60 days, issues involving IG independence, and information on closed investigations, evaluations, and audits that were not disclosed to the public.

Ongoing Report Requested by the House Committee on Oversight and Government Reform

The OIG responded to a letter signed by Representative Jason Chaffetz, Chairman of the House Committee on Oversight and Government Reform, and by Representative Elijah Cummings, the Committee's Ranking Member, requesting several items of information on a continuing basis. Our response included information on outstanding unimplemented audit recommendations (including those the IG felt most important or urgent), and information on closed investigations, evaluations, and audits that were not disclosed to the public.

Federal Records Issue Response

The OIG continued to provide congressional staff with information concerning an ongoing issue surrounding Federal records of a past Secretary of State.

NARA Research Room Complaint

The OIG responded to a Senator's office concerning questions about a constituent's complaint about NARA actions in a NARA research room.

The Government Charge Card Abuse Prevention Act of 2012

At a minimum the OIG is required to conduct annual assessments of the agency's purchase card program, and analyze or audit, as necessary, purchase card transactions. We reviewed risks and controls previously identified, received input from NARA staff, and reviewed prior reports (including open recommendations). We also reviewed data on the number of card holders, limits, amounts, and number of transactions. During this process, we reviewed and updated a risk assessment of NARA's purchase card program. We assessed the risk over NARA's purchase card activity as moderate based on the number of card holders and the amount purchased with the cards. We determined, except for some related open recommendations, NARA has effective policies, procedures, and monitoring controls.

Audit and Reports Overview

During this reporting period, the OIG hired Assistant Inspector General for Audits (AIGA) Jewel L. Butler to lead the Office of Audits (OA). AIGA Butler has more than 15 years of Federal audit experience, including at the U.S. Department of Agriculture OIG and the Department of Homeland Security OIG. AIGA Butler brings with her the experience to enhance OA operations and ensure our audit work continues to foster positive change throughout the agency.

Also, during this reporting period we issued five final audits, and initiated or continued work on audits or reports of:

- NARA's Compliance with Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification standard for Federal Employees and Contractors, determining whether NARA is effectively complying with HSPD-12 requirements for accessing agency facilities and information systems;
- NARA's Procurement Program, determining whether NARA's procurement program is efficient and effective for acquiring goods and services providing the best value to NARA;
- NARA's Refile Processes at Selected Federal Records Centers (FRCs), assessing the effectiveness and adequacy of management controls in place for refiles of Internal Revenue Service records at six FRCs;
- An enterprise-wide risk assessment of internal controls and associated risks to NARA's mission, operations, and procedures by an independent contractor ;
- NARA's Preparation and Planning for the Receipt of the Obama Administration's Records and Artifacts, assessing the adequacy and appropriateness of these efforts;
- NARA's Management Control over Microsoft Access Applications, identifying the Access applications in use; assessing security controls; and determining whether NARA is appropriately positioned to accommodate and maintain the applications;
- NARA's Compliance with the Improper Payments Elimination and Recovery Act of 2010;
- NARA's Compliance with the Federal Managers Financial Integrity Act (FMFIA) for FY 2015, OMB Circular A-123, and NARA-developed internal control guidance;
- NARA's Inventory System Tracking and Monitoring Process, determining if NARA has developed a comprehensive information system inventory to track and monitor all

information systems and whether all NARA systems have been classified and categorized as required; and

- NARA's policies and practices related to covered systems as required by the Cybersecurity Act of 2015.

Audit Summaries

Audit of NARA's Web Hosting Environment

NARA describes its core mission as providing public access to Federal records. The first goal of NARA's 2014-2018 Strategic Plan, "Make Access Happen," states its objective is to "make all records available to the public in digital form to ensure that anyone can explore, discover, and learn from NARA holdings." However, this cannot adequately occur without NARA's website infrastructure, including NARA's public facing websites and the environments hosting them. The objective of this audit was to determine if NARA maintains a secure web hosting environment.

We found NARA does not provide consistent oversight and management of the agency's public facing websites and web hosting environments. NARA entities were able to create websites without management's approval or knowledge, resulting in an inventory of websites and web hosting environments with greater susceptibility to security and legal vulnerabilities. By not knowing how many websites are managed by NARA entities, its vendors, or partners; or where those websites are hosted, NARA has reduced assurance whether all of the public facing websites the agency is responsible for are actually secure.

Further, the Office of Innovation did not classify or categorize NARA's internal web hosting environment in accordance with Federal information security standards. These processes are necessary for developing and implementing appropriate security controls. We also found numerous control weaknesses within NARA's internal web hosting environment. As a result, NARA cannot ensure information security protections are in place commensurate with the risk to the confidentiality, integrity, and availability of NARA's internal web hosting environment.

In addition, NARA did not require external vendors or partners to conduct and provide security assessments of the systems hosting NARA's websites. As a result, NARA's ability to ensure the agency's external web hosting environments are adequately secure and compliant with Federal security standards is severely inhibited, and NARA loses the ability to adequately control and secure IT information hosted on the websites. Should these websites be compromised, NARA has no insight or ability to fix them. The report made 33 recommendations to improve NARA's security of internal and external web hosting environments, management over public facing websites, communication between NARA organizations, and Federal Information Security Management Act compliance. (OIG Audit #16-01, dated October 19, 2015.)

Audit of NARA's Compliance with the Federal Information Security Modernization Act (FISMA) for FY2015

FISMA requires annual independent evaluations of the effectiveness of NARA's information security practices. We contracted with an independent public accounting firm (IPA) to complete the evaluation and provide an audit report. The evaluation found efforts were made to address some of weaknesses identified from previous FISMA evaluations and audit engagements. Specifically, NARA's Incident Response and Reporting program, one of the 10 functional areas for evaluation, was determined to be in accordance with FISMA requirements, OMB policy, and National Institute of Standards and Technology (NIST) guidelines. However, NARA still needs significant improvement in other areas to be consistent with FISMA and NIST guidance. The IPA found controls weaknesses including the following:

- Risk assessment controls (1 control weakness)
- Security configuration baseline implementation controls (1 control weakness)
- Account management controls (6 control weaknesses)
- Plans of action and milestones process (1 control weakness)
- Update of system security plans (3 control weaknesses)
- Security controls on patch and configuration management (2 control weaknesses)
- Controls over role-based training (1 control weakness)
- Contingency planning controls (4 control weaknesses)
- Controls over audit logging (3 control weaknesses)

The Chief Information Officer (CIO) indicated these weaknesses represent long-standing issues in NARA's security environment. Specifically, the CIO attributed these to: (a) inadequate management resources and budget for many years; (b) lack of effectively implemented processes and procedures; and (c) corrective actions which require long term solutions. These issues potentially expose NARA's information and information systems to unauthorized access, use, disclosure, disruption, modification, or destruction. The audit made 20 recommendations.

Audit of NARA's Publicly Accessible Websites

Website vulnerabilities have become a point of emphasis for attackers trying to access an organization's information technology infrastructure. Securing publicly-accessible websites is critical to ensuring the security and accessibility of NARA's network. We evaluated the security of NARA's publicly-accessible websites. In addition, we assessed NARA's progress toward implementing secure hyper text transfer protocol (HTTPS) on all government websites as required by the OMB. We also evaluated whether NARA had proper controls in place to ensure security assessments for cloud hosted websites were reviewed prior to a contract being signed. We found NARA's publicly-accessible websites are not adequately secured and properly protected. NARA has not provided adequate management oversight nor implemented strong or effective internal controls to ensure the security of its publicly-accessible websites. We identified numerous security deficiencies in NARA's publicly-accessible websites including, but not limited to the following:

- NARA has not developed sufficient security control guidance for websites
- NARA has not fully implemented website vulnerability scanning
- NARA websites are vulnerable to a specific type of action
- NARA does not protect the confidentiality of the passwords used on its websites
- Information within NARA websites provide attackers with insight into sensitive files and folders within NARA websites and employee information.

NARA has not securely and consistently configured HTTPS on its websites. We identified 14 websites currently implementing HTTPS, and found 9 of these websites do not meet federal guidelines for secure HTTPS configuration. NARA has not developed any guidance to ensure HTTPS is securely and consistently configured on its websites. As a result, NARA is not providing the strongest privacy and integrity protection available to its users as required by OMB.

We also found security assessments for cloud web hosting providers were not reviewed. NARA does not have a standard process in place to review security assessments performed on cloud web hosting environments. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Government Accountability Office (GAO) Standards require management to evaluate and document the results of ongoing monitoring and separate evaluations to identify internal control issues. Management should use this evaluation to determine the effectiveness of the internal control system. By not evaluating the security assessments, NARA lacks assurance the agency's cloud web hosting environments are adequately secured and compliant with FISMA. The report makes seven recommendations to improve the security surrounding NARA's publicly-accessible websites. (OIG Audit #16-05, dated March 25, 2016.)

NARA's Inadequate Information and Physical Security Controls at Select Federal Records Centers (FRCs)

This audit was initiated to assess the effectiveness and adequacy of management controls for the refile processes at selected FRCs. However, 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 the Lee's Summit and Lenexa FRCs. This report focuses on the information and physical security findings noted during the audit.

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).[1] Lee's Summit maintains electronic tracking and inventory systems 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

[1] U.S. Customs & Border Protection, U.S. Citizenship & Immigration Services, and U.S. Immigration & Customs Enforcement.

to protect PII. There were issues in areas 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 employee's PII highlighted the significance of ensuring proper safeguards are implemented to prevent similar attacks.

Special media records are NARA holdings such as film, sound, and video recordings; and still pictures. After a theft of many special media records by a NARA employee, additional holdings and physical security controls were implemented at some NARA offices.[2] However, some weaknesses still exist. 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. Lenexa's cold storage facility, which was separated from the main facility, had insufficient controls in place to safeguard special media records. Weaknesses included the lack of monitoring of entry and exit activity, an updated key log, and a properly secured door to 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 with Information Security management after the OIG identified the information security weaknesses.

Overall, the 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.

NARA's FY 2015 Financial Statements Independent Audit Report

We contracted with CliftonLarsonAllen LLP (CLA), a public accounting firm, to audit NARA's Consolidated Balance Sheets as of September 30, 2015, and the related Statements of Net Cost, Changes in Net Position, and Budgetary Resources. NARA was issued an unmodified opinion on its FY 2015 financial statements. There was one significant deficiency in internal control over financial reporting related to information technology. No material weaknesses or instances of noncompliance with certain provisions of laws and regulations were discovered. There was one recommendation.

We monitored CLA to ensure the audit was conducted in accordance with the contract, and in compliance with the Government Accountability Office's *Government Auditing Standards* and other authoritative references, such as OMB Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. Our review disclosed no instances wherein CLA did not comply, in all material respects, with the contract or *Government Auditing Standards*. (OIG Audit Report #16-04, dated December 21, 2015.)

[2] The former employee was sentenced in 2012 for stealing sound recordings from NARA during his employment.

Investigations Overview

The Office of Investigations (OI) receives and evaluates complaints, and conducts investigations related to fraud, waste, and abuse in NARA programs and operations. This includes identifying and recovering wrongfully alienated NARA holdings. Investigations showing violations of law, regulations, rules, or contract terms may result in administrative, civil, or criminal actions. These can include things such as terminations, debarments, prison terms, probation, fines, or restitution. The OI may also issue management letters detailing specific problems or vulnerabilities, and offering insight on how to correct them.

Significant Investigations

Partner Contractor Destroying Federal Records (conclusion)

Previously we reported a contract employee had mutilated and destroyed World War II-era Selective Service System records and Draft Registration Cards, rather than processing them in accordance with the terms of the contractor's partnership agreement with NARA. In September 2015, the (former) contract employee pleaded guilty to one charge of destroying Federal records. In this reporting period, in December 2015, the Federal court sentenced him to three years of supervised probation, a special assessment of $100, and restitution to NARA in the amount of $13,399.96.

NARA's Public Transit Subsidy Program (PTSP) (conclusion)

Previously we reported that some NARA employees were uninformed of many of the important rules on the Public Transit Subsidy Program, and were breaking the rules without meaning to. In response to our Management Letter explaining the problems, the agency agreed to (1) include policy reminders and a direct link to the policy in future recertification reminders, (2) update the annual ethics training to include a Public Transit Subsidy Program scenario, and (3) provide training to managers and supervisors highlighting their oversight and reporting role.

In addition to the Management Letter, our investigation resulted in the presentation of three subjects to the Office of the United States Attorney for criminal prosecution. However, prosecution for all three subjects was declined in favor of administrative remedy. The OI issued a Report of Investigation and potential disciplinary action from the agency is pending.

Employee Secretly Tape-Recorded Discussion with Supervisor

We received an allegation a NARA employee in Maryland had secretly tape-recorded a workplace conversation among themselves, their supervisor, and several other employees. This may have been a violation of Maryland state law which prohibits recording private conversations without consent. Our investigation determined the employee did record the meeting, as alleged. The case was presented to the Office of the State's Attorney for Prince George's County, Maryland, which declined prosecution. The results of this investigation were referred to NARA for any action deemed necessary.

False Information on Employment Application Documents

We reviewed allegations an employee submitted false information in their employment application documents, including information pertaining to termination from previous employment, criminal arrest history, and other issues. The investigation substantiated the allegation, and the employee was referred for criminal prosecution. Both the Federal and Maryland prosecutors declined prosecution in favor of administrative action. The OI issued a Report of Investigation and potential disciplinary action from the agency is pending.

Employee Used Researcher Application to Obtain Contact Information for Social Interaction

We substantiated an allegation a NARA employee inappropriately accessed researcher application documents for contact information for private use. Our investigation established the employee abused his position to obtain a researcher's contact information, and then sent the researcher an email soliciting social interaction. The incident was referred for to the Office of the United States Attorney, which declined to prosecute in favor of administrative action. In response to our Report of Investigation, the employee received a letter of reprimand.

Unauthorized Outside Employment in the Workplace

We reviewed an allegation an employee operated a private business in the workplace, selling jewelry to contractors and fellow employees. The investigation substantiated the allegation, showing the employee had not submitted a mandatory disclosure/request/permission form for outside employment, and had used NARA information technology resources to advertise their business. Further, the employee provided incomplete and misleading information to investigators. The OI issued a Report of Investigation, and potential disciplinary action from the agency is pending.

Significant Referrals

Government Travel Card Canceled After 120 Days' Delinquency in Payment

A supervisor failed to pay charges totaling approximately $1,200 on their Government travel card. After 120 days' delinquency, the card was cancelled and the matter was referred to the OIG and to the Labor/Employee Relations and Benefits Branch for disciplinary action. A review found the non-payment resulted from multiple circumstances, including unclear travel system processes and requirements. These can be addressed with additional training and greater familiarity with the travel system. The employee was given a letter of reprimand.

Alienated Presidential Pardons Recovered for NARA

An auction house contacted the OIG to report an upcoming auction collection contained seven pardons issued by U.S. Presidents and appeared on NARA's online list of lost or stolen documents (see http://www.archives.gov/research/recover/). Research Services, the Office of the General Counsel, and the Office of the Chief Operating Officer worked with the auction house to have the documents removed from the upcoming auction, and were able to establish they actually were alienated NARA property. The Office of the General Counsel worked with the auction house to support NARA's formal claim to the documents, which were returned to NARA on January 22, 2016.

IT Equipment Decommissioned and Surplussed But Not Purged of NARA Content

A private citizen reported his recent *eBay* purchase of a NARA-surplussed network router switch (the device) still contained a NARA configuration file. Although the device had not yet reached the end of its service life and should not have been surplussed, NARA did surplus it to the

General Services Administration, which sold it on *eBay*. While this matter was reviewed NARA implemented appropriate security measures and put a freeze on the surplus process for similar devices. The review showed an additional 16 electronic items had been surplussed without first being sanitized of NARA content, and highlighted the specific procedural weaknesses that allowed it to happen. No intentional wrongdoing was discovered. NARA has revised its decommissioning procedures to ensure future equipment is not prematurely decommissioned or surplussed in this manner.

Alienated Military Records Recovered for NARA

We reviewed an allegation an auction site was going to sell military records appearing to be NARA property. We found the records were part of a veteran's military personnel file from the U.S. Army Air Force's Motion Picture Unit. The veteran had served alongside future President Ronald Reagan, and all of the documents bore then-Lieutenant Reagan's signature. The auction site had obtained the documents from the veteran's estate, but we were unable to determine how the veteran himself had originally obtained them or when. Our investigation established the documents were, or should have been, part of the veteran's official military personnel file, and were therefore the property of the United States Government. Representatives of the Office of the Chief Operating Officer were involved in the document recovery. Six documents were recovered, and are now in NARA custody.

Ongoing Oversight

The National Personnel Records Center (NPRC) responds to requests for veterans' records from veterans, their next of kin, and various other requesters. A typical NPRC correspondence technician responds to approximately 1,000 requests in a two month period. On occasion, responses can contain the records of the incorrect veteran (i.e. for similar names, etc.), and some veterans' files may contain the records of others, including their PII. The NPRC tracks these occurrences when they are notified, and uses progressive discipline as they deem appropriate when the root cause is determined to be technician carelessness. The NPRC sends a monthly report to the OIG providing detailed information on each instance of accidental erroneous release. In this period, the OIG noticed the same user name appeared on the report for two consecutive months. We sent the NPRC a referral about this individual, they responded by providing a copy of a counseling letter which had already been issued to the employee.

OIG Hotline

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number and letters to the Hotline post office box, we also accept emails through the Hotline email system and an online referral form. Walk-ins are always welcome. Visit *http://www.archives.gov/oig/* for more information, or contact us:

- **By telephone**
  Washington, DC, Metro area: (301) 837-3500
  Toll-free and outside the Washington, DC, Metro area: (800) 786-2551
- **By mail**
  NARA OIG Hotline
  P.O. Box 1821
  Hyattsville, MD 20788-0821
- **By email**
  oig.hotline@nara.gov
- **By facsimile**
  (301) 837-0879
- **By online referral form**
  http://www.archives.gov/oig/referral-form/index.html

The OI promptly and carefully reviews calls, letters, and email to the Hotline. We investigate allegations of suspected criminal activity or civil fraud and conduct preliminary inquiries on noncriminal matters to determine the proper disposition. Where appropriate, referrals are made to OIG audit staff, NARA management, or external authorities.

Hotline Activity for the Reporting Period	
Hotline and Complaints received	168
Hotline and Complaints referred to NARA or another entity	53

Contractor Self Reporting Hotline

As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at *http://www.archives.gov/oig/contractor-form/index.html*.

Disagreements with Significant Management Decisions

Under the IG Act, as amended, the OIG reports "information concerning any significant management decision with which the Inspector General is in disagreement." The following disagreements have been reported previously, but as nothing has changed, they remain an issue.

In October 2015, we reviewed NARA's FY 2015 Draft Federal Managers' Financial Integrity Act (FMFIA) statement. We disagreed with the assurance statement for Section 2 of the FMFIA reporting requirements. We disagree because the current entity-wide Internal Control Program is not comprehensive nor developed enough to clearly reflect NARA's internal control environment. Without a fully implemented program that is able to identify, document, and test risks and controls for each function, the agency is not able to identify all its existing risks and potential weaknesses. The agency assurance statement currently underreports material weaknesses and does not accurately reflect the breadth of risks in NARA's Holdings Protection, Processing, Electronic Records Management, and Information Security Programs.

NARA's Holdings Protection Program

NARA's FY 2014 assurance statement downgraded the Holdings Protection Program from a material weakness to a reportable condition. The agency based this decision on (1) the development and application of risk-ranking criteria for facilities and (2) a gap analysis of actions taken since the program was declared a material weakness 13 years ago. According to the agency, the analysis identified no material control gaps.

Based on our assessment, the two actions presented by the agency are no basis for the downgrade. Specifically, based on our review of the analysis, a majority of the identified Holdings Protection internal controls have material gaps for internal threats, external threats, and specially protected records. We also noted none of the internal controls identified in the analysis were mapped to risks or risk-ranked (high, medium, low). There was limited supporting documentation provided to support both actions, including the review and testing of the controls.

Further, there is also confusion in the agency over the Holdings Protection Team's real mission and how the Team will best execute the mission in the future. This is evident by the Team's failure to perform proactive analyses aimed at strengthening protection of NARA's holdings. These issues and continued concerns over the program are driving the OIG to plan an entity-wide holdings protection audit.

NARA's Processing Program

NARA's FY 2012 assurance statement downgraded the processing program from a material weakness to a reportable condition. The agency made this decision based on the current state of Federal records processing, the strides the agency has made in the last six years, and the current focus on reengineering processing work. The agency also decided to remove the processing of electronic Presidential records from this weakness since the processes and requirements for processing these records are distinctly different from Federal textual records.

Based on our assessment, NARA's processing program should still be carried as a material weakness. Approximately 28 percent of NARA's textual holdings have not been processed, which will not allow efficient and effective access to these records. Further, in our FY 2013 audit[3] we reported the strategic direction of processing needs to include an overall agency policy and definition, adequate backlog reduction plans for Research Services field locations, plans for increased processing progress in the Presidential libraries, improved processing staff utilization, and a realistic and attainable processing goal. Some of the actions planned by the agency to address the critical recommendations were scheduled to be completed in FY 2015, but have been rescheduled to be completed in FY 2016. Therefore, the risks identified in the audit report still exist. As a result, a processing backlog continues placing records at risk, increasing the time for reference requests, impairing the agency's ability to describe the records online, and limiting access to records.

NARA's Information Systems and Technology Security (IS&TS)

Since our last review of this issue NARA has reassessed its IS&TS, and has declared a material weakness in IT security in five areas. This admission is an encouraging start and our office looks forward to NARA's efforts to correct this situation. However, as stated before, our reviews have found critical functions, controls, and risks for IS&TS have not been adequately identified, making it difficult to assess the control environment for IS&TS. Our previous audits (e.g., Network Discovery and Assessment, Network Vulnerability Assessment and Penetration Testing, Wireless Access, and Assessment of Cable Infrastructure [4]) and NARA's internally contracted studies continue to point to internal control weaknesses, including the potential for NARA's network to be hacked. These may extend beyond the five areas NARA has identified. Findings from the OIG's FY 2013 Federal Information Security Management Act (FISMA) assessment[5] where we reported the agency did not have an established program in any of the 11 assessment areas, should help guide NARA's efforts.

NARA's Electronic Records Management Program

NARA reported the Electronic Records Management program as a reportable condition instead of a material weakness. According to NARA, this was based on the fact the President issued a memorandum and subsequently NARA and OMB jointly issued Memorandum 12-18, *Managing Government Records Directive*. These documents represent an executive branch-wide effort to reform records management policies and practices and to develop a 21st-century framework for the management of government records. Management is using Memorandum 12-18 to guide the development of the Chief Records Officer operational plans for years to come and serve as an action plan against which NARA can monitor and assess progress. However, the directive does not mitigate the existing risks outlined in our 2010 audit report, OIG 10-04, *NARA's Oversight of*

[3] Audit Report No. 13-14, Audit of Processing Textual Records, dated September 18, 2013.

[4] Audit Report No. 12-11, IMRI Network Discovery and Assessment Report dated August 27, 2012, Audit Report No. 11-05, Clifton Gunderson LLP Network Vulnerability Assessment and Penetration Testing dated November 8, 2010, Audit Report No. 14-10, Cotton & Company's Audit of NARA's Enterprise Wireless Access dated May 9, 2014, and Audit Report No. 15-15, Cotton & Company's Assessment of NARA's Cable Infrastructure, dated September 30, 2015.

[5] Audit Report No. 15-01, NARA's Information Security Program, dated October 27, 2014.

SIGNIFICANT DISAGREEMENTS

Electronic Records Management in the Federal Government. The report found NARA did not have adequate controls in place to protect permanent Federal electronic records from loss. Specifically, we reported NARA could not reasonably ensure permanent electronic records are being adequately identified, maintained, and transferred to NARA in accordance with Federal regulations. Until sufficient controls have been implemented to minimize these risks, NARA should classify this program as a material weakness.

GAO conducted a review to assess Federal agencies implementation of Memorandum 12-18, including actions taken by NARA to assist agencies in using electronic recordkeeping and ensuring agencies comply with Federal records management statutes and regulations. We reviewed GAO's audit and do not believe the material weakness can be downgraded.

SEP 5 1933
No. 40 Taken Sept. 5 1933
The Archives Building
Washington, D. C.
John Russell Pope, Architect
George A. Fuller Co., Builders

Overview

Under the authority of the Inspector General Act, the NARA OIG conducts and supervises independent audits, investigations, and other reviews to promote economy, efficiency, and effectiveness; and to prevent and detect fraud, waste, and mismanagement. To fulfill our mission and help NARA achieve its strategic goals, we have aligned our programs to focus on areas we believe represent the agency's most significant challenges. We have identified those areas as NARA's top ten management challenges.

1. Electronic Records Archives

The Electronic Records Archives (ERA) system is a repository for electronic Presidential, Congressional, and Federal agency records that stores files in any format for future access. The ERA system is NARA's primary strategy for addressing the challenge of storing, preserving, transferring and providing public access to electronic records. However, virtually since inception the program has been fraught with delays, cost overruns, and technical short comings and deficiencies identified by our office and the Government Accountability Office (GAO). As a result, many core requirements were not fully addressed, and ERA lacks the originally envisioned functionality.

The ERA Base System for Federal electronic records has had many problems with its reliability, scalability, usability, and cost, which have prevented it from being adequate for both NARA's current and expected future workload. Given the limitations of the system in managing the transfer, processing and storage of large deliveries of digital materials, and advances in technology (particularly cloud computing), NARA has determined it is essential to evolve the current ERA Base System. This will entail the correction and re-factoring of current capabilities, as well as the adaptation and expansion of capabilities in order to fulfill the agency's mission to meet the expected demands of a rapidly growing backlog of digital and digitized materials.

ERA faces many challenges ahead. These include the growth in the amount and diversity of digital materials produced by government agencies. Challenges also include the need for expanded capabilities to achieve the mission of driving openness, cultivating public participation, and strengthening the nation's democracy through access to high-value government records. In addition, NARA is planning for a significant number of electronic records from the Executive Office of the President, as the next election in November 2016 will result in a change of administration.

2. Improving Records Management

NARA must work with Federal agencies to ensure the effective and efficient appraisal, scheduling, and transfer of permanent records, in both traditional and electronic formats. The major challenge is how best to accomplish this while reacting and adapting to a rapidly changing technological environment in which electronic records, particularly email, proliferate. In short, while the ERA system is intended to work with electronic records received by NARA, we need to ensure the proper electronic and traditional records are in fact preserved and sent to NARA in the first place.

In August 2012, the Office of Management and Budget (OMB) and NARA jointly issued Memorandum 12-18, *Managing Government Records Directive*, creating a robust records management framework. This directive requires agencies, to the fullest extent possible, to eliminate paper and use electronic recordkeeping. It is applicable to all executive branch agencies and to all records, without regard to security classification or any other restriction. This directive also identifies specific actions to be taken by NARA, OMB, and the Office of Personnel Management (OPM) to support agency records management programs. Agencies must manage all permanent electronic records in an electronic format by December 31, 2019, and must manage both permanent and temporary email records in an accessible electronic format by December 31, 2016. NARA, its government partners, and Federal agencies are challenged with meeting these deadlines, determining how best to manage electronic records in accordance with this guidance, and how to make electronic records management and e-Government work more effectively.

In May 2015, GAO completed a study evaluating Federal agencies' implementation of the directive. They found NARA's plan to move agencies toward greater automation of records management did not include metadata requirements in its guidance, as required. Further, until agencies, OMB, and NARA fully implement the directive's requirements, GAO indicated the Federal government may be hindered in its efforts to improve performance and promote openness and accountability through the reform of records management. Subsequently, NARA did issue metadata guidance in September 2015. However, that is only one aspect of a complicated issue. Until sufficient controls have been implemented to protect permanent Federal electronic records from loss, NARA should classify electronic records management as a material weakness.

3. Information Technology Security

Each year, risks and challenges to IT security continue to be identified. Many of these deficiencies stem from the lack of strategic planning with regard to the redundancy, resiliency, and overall design of NARA's network. These issues not only allow for security and performance problems, but they inhibit NARA IT management from effectively establishing a tactical and innovative strategy for the next generation of NARA's network. NARA must ensure the security of its data and systems or risk undermining the agency's credibility and ability to carry out its mission.

The Archivist identified IT Security as a material weakness under the Federal Managers' Financial Integrity Act reporting process from FY 2007 to FY 2012. In 2013, NARA reclassified and downgraded the material weakness in IT security to a reportable issue. However, in January 2015, NARA decided to again reclassify IT security from a reportable issue back up to a material weakness. We have been informed this material weakness focuses on specific aspects, and does not encompass the entire IT security program. This is concerning, as audits and assessments continually identify that significant improvements and focused efforts are needed to establish a mature information security program. Further, there are identified vulnerabilities which still present an elevated risk to the agency and its sensitive data.

Annual assessments of NARA's compliance with the Federal Information Security Management Act have consistently identified program areas in need of significant improvement. While initiatives have been introduced to promote a mature information security program for the agency, real progress will not be made until NARA establishes an effective system of internal control for information security. The confidentiality, integrity, and availability of our electronic records and information technology systems are only as good as NARA's IT security program infrastructure.

4. Expanding Public Access to Records

NARA's FY 2014-2018 Strategic Plan emphasizes public access to records by including the strategic goal: "Make Access Happen." This goal establishes public access as NARA's core purpose and includes an initiative to digitize all analog archival records to make them available online. Although NARA recently updated the agency's digitization strategy, historically the digitization approaches implemented were not large enough to make significant progress in meeting this goal. Further, due to poor planning and public access system limitations, millions of records digitized through NARA's partnership agreements were not made accessible to the public in an efficient and timely manner. NARA must ensure the appropriate management, controls, and resources are in place to successfully implement its digitization strategy and expand public access to records.

Another challenge for NARA, given society's growing expectation for easy and near-immediate access to information online, will be to provide access to records created digitally ("born digital") and to identify those textual records most in demand so they can be digitized and made available electronically. NARA's system for providing public online access to its electronic records was performing below accepted industry averages for response times, and as designed, this performance will decrease in direct proportion to the amount of content available in the system. This lack of scalability necessitated a new system, referred to as the National Archives Catalog (NAC), which was launched in December 2014. This was the first phase of a multi-year project, with additional functionality planned. The implementation of the NAC's functionality will greatly impact NARA's ability to meet its "Make Access Happen" strategic goal.

Approximately 28 percent of NARA's textual holdings have not been processed to allow efficient and effective access to them. To meet its mission, NARA must work to ensure it has the processes and resources necessary to establish intellectual control over this backlog of unprocessed records. However, NARA's FY 2012 assurance statement downgraded the Processing Program from a material weakness to a reportable condition. This is concerning, as audits have identified multiple issues with the program, including the fact NARA lacks a strategic direction. Further, NARA reports the amount of unprocessed records by giving the percentage of records which have been processed. However, this can lead to un-intuitive results, such as when the physical volume of unprocessed records increases, but the percentage of records processed increases as well since the total collection is growing. Thus an "improving" percentage figure can at times also represent a physically growing backlog of unprocessed records.

5. Meeting Storage Needs of Growing Quantities of Records

NARA is approaching its overall archival storage capacity. Space limitations are affecting NARA's accessioning, processing, preservation, and other internal efforts. NARA is challenged in acquiring sufficient archival space to store its ever-increasing volume of textual records. Without obtaining additional archival space, NARA may face challenges in meeting its mission and may have to house accessioned textual records in space not meeting its physical and environmental requirements. NARA-promulgated regulation 36 CFR Part 1234, "Disposition of Federal Records," Subpart K, "Facility Standards for Records Storage Facilities," requires all facilities housing Federal records to meet defined physical and environmental requirements. NARA's challenge is to ensure NARA's own facilities, as well as those used by other Federal agencies, are in compliance with these regulations; and to effectively mitigate risks to records which are stored in facilities not meeting these standards.

In addition to NARA's physical storage needs, the agency is also challenged in meeting its requirements for electronic data storage. NARA's in-house data storage is reaching capacity, impacting the agency's digitization efforts and other IT programs dependent on scalable, secure, and readily available data storage. Increasing amounts of electronic data storage are necessary for NARA to meet its mission. Without adequate storage NARA cannot continue accepting, storing, and processing records, or make electronic records available to the public. NARA is challenged to develop an enterprise-wide data storage management solution compliant with the Office of Management and Budget's Federal Data Center Consolidation Initiative, which focuses on reducing the energy and real estate footprint of government data centers.

6. Preservation Needs of Records

Preservation continues to be a material weakness for the agency. NARA holdings grow older daily and face degradation associated with time. This affects both traditional paper records and the physical media electronic records and audiovisual records are stored on. According to management, preservation resources have not adequately addressed the growth in holdings needing preservation action. Preserving records is a fundamental element of NARA's duties to the country, as NARA cannot provide access to records unless it can preserve them for as long as needed. The backlog of records needing preservation remains steady. NARA is challenged to address this backlog and future preservation needs, including the data integrity of electronic records. Further, NARA's primary tool for preserving electronic records, the ERA system, has not delivered the functionality necessary to address record format obsolescence (see OIG Challenge #1). The challenge of ensuring NARA facilities meet environmental standards for preserving records (see OIG Challenge #5) also plays a critical role in the preservation of Federal records.

7. Improving Project and Contract Management

Effective project and contract management, particularly for IT projects, is essential to obtaining the right equipment and systems to accomplish NARA's mission. Complex and high-dollar contracts require multiple program managers, often with varying types of expertise. NARA is challenged with planning projects, developing adequately defined requirements, analyzing and testing to support system acquisition and deployment, and providing oversight to ensure effective or efficient results within contracted costs. Currently, IT systems are not always developed in accordance with established NARA guidelines. These projects must be better managed and tracked to ensure budget, scheduling, and performance goals are met.

As an example, GAO reported NARA did not document the results of briefings to its senior management oversight group during the development of NARA's largest IT project, the ERA system. There is little evidence the group identified or took appropriate corrective actions, or ensured such actions were taken and tracked to closure. Without adequate oversight evaluating project progress, including documenting feedback and action items from senior management, NARA will not be able to ensure projects are implemented at acceptable costs and within reasonable time frames. GAO also reports NARA has been inconsistent in its use of earned value management (EVM), a project management approach providing objective reports of project status and early warning signs of cost and schedule overruns. Inconsistent use of key project management disciplines like EVM limits NARA's ability to effectively manage projects and accurately report on their progress. In another example, our office found issues in the process of implementing a Homeland Security Presidential Directive (HSPD-12) compliant logical access control system. The HSPD-12 implementation is a long overdue project. Inadequate planning may not only result in delayed completion, but may also hinder the agency from complying with federal laws and regulations.

Further, GAO has identified Commercial Services Management (CSM) as a government-wide initiative. The CSM initiative includes enhancing the acquisition workforce, increasing competition, improving contract administration skills, improving the quality of acquisition management reviews, and strengthening contractor ethics requirements. Effective contract management is essential to obtaining the right goods and services at a competitive price to accomplish NARA's mission. NARA is challenged to continue strengthening the acquisition workforce and to improve the management and oversight of Federal contractors. NARA is also challenged with reviewing contract methods, to ensure a variety of procurement techniques are properly used in accordance with laws, regulations, and best practices.

8. Physical and Holdings Security

Holdings security continues to be a material weakness for the agency. Document and artifact theft is not a theoretical threat; it is a reality NARA has been subjected to time and time again. NARA must maintain adequate levels of security to ensure the safety and integrity of persons and holdings within our facilities. This is especially critical in light of the security realities facing this nation and the risk our holdings may be pilfered, defaced, or destroyed by fire or other man-made and natural disasters. Not only do NARA's holdings have immense historical and financial value, but we hold troves of national security information as well. NARA's implementation of the Holdings Protection Team and stricter access controls within the past five years has increased NARA's security posture. However, without adequate oversight and accountability, NARA continues to be challenged in implementing an effective Holdings Protection Program.

9. Human Resources Management

NARA's ability to attract, recruit, and retain employees while improving workforce morale is critical to many of the other top management challenges. Human capital is integral to NARA's future as the agency continues to build a modern and engaged workforce, develop the next generation of leaders, and encourage employees to collaborate, innovate, and learn. One of the agency's strategic goals is to *"build our future through our people."* However, the agency has not developed a comprehensive and cohesive approach to human capital management. Adequate policies and procedures have not been developed, updated, and communicated and this makes it difficult to manage human capital effectively and efficiently. Further, NARA does not have one authoritative source providing the latest data to role-based users on all types of workers (federal employee, contractor, and volunteer). The numerous existing systems make it difficult to manage the workforce. NARA is challenged to maintain security, data reliability and accuracy; and to manage personnel data and system access for individuals other than federal employees.

10. Management of Internal Controls

Under OMB Circular A-123, *Management's Responsibility for Internal Control*, management is responsible for establishing and maintaining internal controls to achieve effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. GAO has reported NARA has not established an enterprise risk management capability, thus reducing its ability to anticipate future challenges and avoid potential crises. Currently, the agency has not established an effective internal control program. Thus, NARA is vulnerable to risks that may not be foreseen or mitigated, and it does not have the ability to self-identify and appropriately manage or mitigate significant deficiencies. Establishment of an effective internal control program is critical as it provides several benefits, including:

- improved decision making;
- risk identification, management, and mitigation;
- opportunities for process improvement;
- effective use of budgeted resources; and
- strategic planning.

NARA's challenge is to ensure the agency is in compliance with OMB Circular A-123 and to develop and fully implement an internal control program.

REPORTING REQUIREMENTS

MANDATED BY THE INSPECTOR GENERAL ACT OF 1978, AS AMENDED, AND OTHER LAWS

REQUIREMENT	SUBJECT	PAGE(S)
Section 4(a)(2)	Review of legislation and regulations	4, 7
Section 5(a)(1)	Significant problems, abuses, and deficiencies	2–3, 12–15, 16–18
Section 5(a)(2)	Significant recommendations for corrective action	2–3, 12–15
Section 5(a)(3)	Prior significant recommendations unimplemented	33–48
Section 5(a)(4)	Summary of prosecutorial referrals	16–18, 30
Section 5(a)(5)	Information or assistance refused	32
Section 5(a)(6)	List of reports issued	31
Section 5(a)(7)	Summaries of significant reports	2–3, 12–15
Section 5(a)(8)	Audit Reports—Questioned costs	31
Section 5(a)(9)	Audits Reports—Funds put to better use	32
Section 5(a)(10)	Prior audit reports with no management decision	32
Section 5(a)(11)	Significant revised management decisions	32
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	20–22
Section 5(a)(14)	Reporting on OIG peer review	8–9
P.L. 110-181	Annex on completed contract audit reports	32
P.L. 104-106	Prior fiscal years' open audit recommendations	33–48

SUMMARY OF INVESTIGATIONS AND PROSECUTORIAL REFERRALS

Requirement 5(a)(4)

Investigative Workload	
Hotline and complaints received this reporting period	168
Investigations opened this reporting period	11
Investigations closed this reporting period	5
Investigative Results	
Individuals referred – accepted for prosecution	3
Individuals referred – declined for prosecution	3
Individuals referred – pending prosecution decision	0
Arrest	0
Indictments and informations	0
Convictions	1
Fines, restitutions, judgments, and other civil and administrative recoveries	$13,299.96
Administrative Remedies	
Employee(s) terminated	0
Employee(s) resigned	0
Employee(s) suspended	0
Employee(s) given letter of reprimand or warnings/counseled	1
Employee(s) taking a reduction in grade in lieu of administrative action	0
Contractor (s) removed	0
Individual(s) barred from NARA facilities	0

LIST OF AUDIT REPORTS ISSUED

Requirement 5(a)(6)

Report No.	Title	Date	Questioned Costs	Unsupported Costs	Funds Put to Better Use
16-01	Audit of NARA's Web Hosting Environment	10/19/2015	$0	$0	$0
16-02	Audit of NARA's Compliance with the FISMA- FY 2015	01/16/2016	$0	$0	$0
16-03	Inadequate Information and Physical Security Controls at Select FRC's	03/4/2016	$0	$0	$0
16-04	NARA's FY 2015 Financial Statements Independent Audit Report	12/21/2015	$0	$0	$0
16-05	Audit of NARA's Publically Accessible Websites	03/25/2016	$0	$0	$0

AUDIT REPORTS WITH QUESTIONED COSTS

Requirement 5(a)(8)

Category	Number of Reports	DOLLAR VALUE	
		Questioned Costs	Unsupported Costs
A. For which no management decision has been made by the commencement of the reporting period	0	$0	$0
B. Which were issued during the reporting period	0	$0	$0
Subtotals (A + B)	0	$0	$0
C. For which a management decision has been made during the reporting period	0	$0	$0
(i) dollar value of disallowed cost	0	$0	$0
(ii) dollar value of costs not disallowed	0	$0	$0
D. For which no management decision has been made by the end of the reporting period	0	$0	$0
E. For which no management decision was made within 6 months	0	$0	$0

AUDIT REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE

Requirement 5(a)(9)

CATEGORY	NUMBER	DOLLAR VALUE
A. For which no management decision has been made by the commencement of the reporting period	3	$9,073,842
B. Which were issued during the reporting period	0	$0
Subtotals (A + B)	3	$9,073,842
C. For which a management decision has been made during the reporting period	0	$0
(i) dollar value of recommendations that were agreed to by management	0	$0
Based on proposed management action	0	$0
Based on proposed legislative action	0	$0
(ii) dollar value of recommendations that were not agreed to by management	0	$0
D. For which no management decision has been made by the end of the reporting period	3	$9,073,842
E. For which no management decision was made within 6 months of issuance	3	$9,073,842

ANNEX ON COMPLETED CONTRACT AUDIT REPORTS

Section 845 of the 2008 Defense Authorization Act, Public Law 110-181, requires certain information on completed contract audit reports containing significant audit findings be included as an annex to this report. While the OIG audited the ERA and other contracts during this period, they were generally program audits as opposed to contract audits.

OTHER REQUIRED REPORTS

REQUIREMENT	CATEGORY	SUMMARY
5(a)(3)	Prior significant recommendations unimplemented	See pages 33–48.
5(a)(5)	Information or assistance refused	None
5(a)(10)	Prior audit reports with no management decision	Management has concurred or disagreed with all issued reports.
5(a)(11)	Significant revised management decisions	None
5(a)(12)	Significant management decisions with which the OIG disagreed	See pages 20–22.

Prior Fiscal Years' Open Audit Recommendations[6]

Report	Title	Recommendation	
06-09	**Review of NARA's Information Security Program**		
		2a	The Assistant Archivist NH should document policies and procedures for ensuring that software products running on NARANet are current versions, still supported by the software vendors.
06-10	**Evaluation of NARA's Affiliated Archives Program**		
		3	The Archivist should take appropriate measures to revise MOUs between NARA and affiliates to incorporate current standards for housing NARA records.
		4	The Archivist should ensure that there is a mechanism to update the MOUs. Specifically, a procedure should be established to update the MOUs on an interim basis, or when new standards are implemented at NARA.
		5	The Archivist should ensure that all MOUs contain the required clause for the use of the NARA seal.
		6	The Archivist should ensure that all affiliates meet the current storage standards or provide waivers and time frames to have the affiliates become compliant with the NARA 1571 standards.
06-11	**Audit of System Adm. Rights and Controls**		
		5	Ensure that Access Control lists are produced for all IT systems and used as a basis for access validation.
08-01	**Audit of NARA Artifacts**		
		1b	The Assistant Archivist for Presidential Libraries (NL) should ensure that the results of the completed physical inventory are transmitted to NL and appropriately secured to serve as control or master copies establishing a reliable baseline for each library's museum collection.
		2c	The Assistant Archivist for Presidential Libraries (NL) should ensure policies and standards are developed for linking digital images of items to their record in i/O, giving priority to photographing HVOs and outgoing loan items.
		5d	Procure storage hardware appropriate for both the type of artifact and seismic zone; and better configure the museum storage area in order to minimize damage to the artifacts and improve the ease of access to them.
08-02	**Audit of NARA's Purchase Card Program**		
		13	The Assistant Archivist of Administration should direct the Director NAA to establish written policies and procedures to evaluate the effectiveness of cardholder reconciliations and approving officials' certifying duties.
08-05	**FY 07 FISMA Review**		
		7	The Assistant Archivist for Information Services should add security vulnerabilities identified during the server audits to the system's plan of action and milestones to ensure proper tracking and visibility.
		8	The Assistant Archivist for Information Services should conduct "lessons learned" meetings in accordance with the guidance in NIST SP 800-61 when a major incident occurs and periodically for lesser incidents, and develop and implement a control mechanism to verify compliance.

[6] The OIG is currently reviewing documentation submitted by NARA for multiple recommendations listed in this section in order to determine whether the recommendations can be closed.

14 The Assistant Archivist for Information Services should develop and implement a mechanism to monitor system accreditations for NARA's National Security Systems to ensure the systems are re-certified and accredited at least every three years.

16c The Assistant Archivist for Information Services should update the contingency plans, if needed, and record any changes made in the Record of Changes section of the plans.

19 The Assistant Archivist for Information Services should develop a process to identify employees with significant security responsibilities.

08-07 Audit of the Researcher ID Card Program

3 Require periodic monitoring of the Archives I and Archives II database. A log recording the date of the review and corrective action taken should be maintained.

09-15 Audit of NARA's Work at Home System

7 We recommend the CIO ensures that the WAHS meets OMB and NIST requirements prior to full implementation.

09-16 Audit of Processing and Safeguarding Veterans Requests

1 The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to export data for the “record of disclosure file” and follow the approved Records Disposition Schedule and limit the amount of record requests stored online.

3 The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to establish controls to restrict users to only those rights and views needed to perform their job.

6 This audit recommendation contains information concerning an ongoing weakness which could be used to compromise veterans’ information or to exploit NARA programs, operations, and systems if made public. Contact the OIG if you need more information.

7 The Assistant Archivist for Information Services should encrypt backup tapes containing PII as required by OMB Memorandum 06-16.

10-04 Audit of NARA's Oversight of Electronic Records Management in the Federal Government

2 The Archivist should consider using the authority given under Title 44 of the US Code to direct Federal agencies to perform assessments of their electronic records management programs based on requirements contained in 36 CFR Part 1236.

3 The Archivist should ensure NARA establishes a strategy for consistently and systematically monitoring compliance with electronic records regulations and guidance throughout the Federal Government.

4 The Assistant Archivist for Records Services, Washington, DC, (NW) should ensure NARA's strategy for monitoring and evaluating Federal agency compliance with electronic records management regulations and guidance results in adequate identification and mitigation of risks to permanent electronic records.

5 The Assistant Archivist for Records Services, Washington, DC, (NW) should ensure development of controls to adequately monitor agency scheduling of electronic records in an effort to reasonably ensure electronic records/systems are scheduled in timely manner, and therefore provide a reasonably accurate reflection of the universe of electronic records.

6 The Assistant Archivist for Records Services, Washington, DC, (NW) should ensure a methodology for verifying the accuracy/completeness of Federal agency responses to electronic records scheduling requirements resulting from the E-Government Act of 2002.

7 The Assistant Archivist for Records Services, Washington, DC, (NW) should ensure development and application of a methodology for adequately identifying gaps in electronic record accessions. This methodology should reasonably ensure permanent electronic records are identified, scheduled, and ultimately obtained by NARA.

10-07 Audit of NARA's Network Infrastructure

10a The CIO should implement multifactor authentication for network access to infrastructure devices.

14 The Archivist should direct the Assistant Archivist for Information Services, Assistant Archivist for Regional Records Services, and the Assistant Archivist for Presidential Libraries to coordinate with the Assistant Archivist for Administration to develop a mechanism to track access reviews and key inventories for computer rooms and other locations where IT network infrastructure equipment is stored at the field sites.

10-14 Audit of the Process for Providing and Accounting for Information Provided to Researchers

1 The Assistant Archivist for NW should establish formal written policies and procedures to improve NW monitoring of the pull and refile process.

2 The Assistant Archivist for NW should implement a centralized database for all of the NW divisions involved in the processing of researchers' requests for records and determine the necessary information that should be included in the database.

11-02 Network and Penetration Testing Oversight

1 NARA management should apply the appropriate hot fix referenced in the vendor advisory on the affected machines.

2a This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

2b This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

2c This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

3a This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

3b This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

3c This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

3d This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

6a NARA management should immediately address corrective action for all vulnerabilities identified as "high" and "critical" risk.

6b NARA Management should evaluate the identified risks and corrective actions to address those identified as "medium" and "low" risk vulnerabilities.

11-05 Audit of Archives I & II Guard Service Contract

6 The Assistant Archivist for Administration should develop a new fitness standard to test the physical fitness of the security officers that more closely resembles the requirements of the contract.

11-14 Audit of NARA's Foreign and Premium Travel

2a Develop and implement a mandatory specialized training course for travelers and authorizing officials reiterating their roles and responsibilities. Refresher courses should be provided on a periodic basis.

2d Develop and implement procedures to follow up on travel vouchers not submitted within five working days. Take appropriate action for people who do not comply within five working days.

6a Review and update policy and procedures for issuing travel cards to employees. Include additional restrictions as outlined in OMB Circular A-123 on cardholders with credit scores less than 660.

6b Enhance procedures to perform timely periodic reviews of the appropriateness of individually and centrally billed travel cards to help ensure the effectiveness of travel card expenditures controls. Specifically, as outlined in OMB Circular A-123 review ATM cash withdrawals for reasonableness and association with official travel.

11-15 Audit of NARA's Drug Testing Program

2 Amend NARA TDPs to ensure compliance with the SAMHSA’s Interagency Coordinating Group Executive Committee Guidelines for the Selection of Testing Designated Positions and establish a mechanism to periodically review and update TDPs as necessary.

3 Develop a training course for all supervisors that will aid them in recognizing and addressing illegal drug use by agency employees. This training should be mandatory for all supervisors. Also evaluate the current drug awareness training for employees.

4 Develop a retention plan for all drug testing-related documentation consistent with the guidance issued by SAMHSA.

5 Review NARA's Drug Free Workplace Plan and update it as necessary. In addition, a plan for periodic reviews and updates of the plan document should be developed.

11-20 Audit of NARA's Telework Program

1d Develop a method and common criteria for tracking telework participation.

3a The Executive for Information Systems, CIO, and Executive for Business Support Services should ensure all deferred and failed security tests have been reassessed and the results documented.

3e Review Citrix security configurations for adequacy.

12-02 Audit of the Management of Records at the Washington National Records Center

14b This audit recommendation contains information concerning security deficiencies in NARA's handling of national security classified materials, and has not yet been made publicly available.

12-05 Audit of the Management of Records at the Washington National Records Center

3a A Problem Resolution Process is created for all problems, regardless of whether they are considered major or minor. All problems should be tracked to resolution and supported by adequate documentation.

3b A mechanism to facilitate the problem tracking and resolution process is implemented.

5 The Executive for Agency Services should ensure a process to perform periodic inventories of the records held at WNRC is documented and implemented. This process should be systematic and repeatable.

6b A detailed review of the record storage areas is performed to assess the conditions of records stored at WNRC. Problems identified should be corrected.

7 The Executive for Agency Services should ensure accounts for separated or terminated employees are terminated in a timely manner. Also quarterly reviews of access to ARCIS should be performed to identify whether user accounts access is appropriate.

8 The Executive for Agency Services should ensure management designs and implements monitoring activities for records processed at WNRC including weekly, monthly, and quarterly reports.

9c A monitoring process is implemented for ensuring classified operations are performed as written in the Classified SOP.

12a Procedures for all WNRC processes are documented. Review existing procedures and update as necessary.

12b Procedures between unclassified and classified processes are consistent where possible.

12-09 Audit of NARA's Data Center Consolidation Initiative

1b The CIO should update the Master System List and/or Enterprise Architecture to incorporate energy usage calculations.

1c The CIO should update the Master System List and/or the Enterprise Architecture to incorporate realistic estimates of funding needed or savings to be realized from implementing NARA's data center consolidation goals.

1d The CIO should update the Master System List and/or the Enterprise Architecture to incorporate annual savings metrics such as rack count reduction, server count reduction, energy usage reduction, and energy cost reduction to monitor progress.

3 The CIO should conduct the consolidation/virtualization analysis to investigate the impact of consolidating or virtualizing two major application domains (NISP and ERA) and the General Support System (NARANET) as planned, or evaluate other alternatives to increase the average server utilization rate.

4 The Executive for Business Support Services should evaluate the current organization of rack space and determine whether servers can be consolidated into fewer racks when considering space optimization, power consumption, operations management, and component failure/recovery perspectives.

5 The CIO should review and approve the annual Enterprise Architecture update to ensure that the agency is considering OMB's cloud-first policy and guidance on virtualization and consolidation.

12-10 Follow up Audit of Artifacts

1a The remaining five libraries complete baseline inventories as expeditiously as possible with master copies forwarded to LP.

1b The remaining five libraries performing baseline inventories complete legacy reconciliation to identify discrepancies as expeditiously as possible and all libraries with identified discrepancies take action to resolve the discrepancies.

1c Ensure the Reagan Library has taken all appropriate action to resolve the 1,700 identified anomalies in order to complete Recommendation 5b from prior audit report OIG #08-01.

1f Photographs of all valuable and vulnerable (V/V) artifacts and artifacts on loan are completed, and all libraries establish plans to photograph their remaining collection.

1h Appropriate storage hardware for the Reagan Library is procured and installed.

2a Develop and identify an appropriate staffing plan for museum operations. The plan should 1) align with collection sizes and life cycles, (2) include temporary staff or other staffing alternatives to support collection inventories and other core collection work, and (3) identify the planned inclusive time periods devoted to the collection inventory.

2b Review and revise current time-guidance policy, as appropriate, for baseline inventories for newly established Presidential libraries.

5b Develop documentation guidelines that identify the importance of supporting the conclusion reported on the annual V/V reports. When counting objects, the support documentation should show the same count.

7a Policies and procedures are clarified and reiterated to library personnel concerning 1) sequestration of museum artifacts from library personnel other than museum personnel, and 2) procedures to periodically review access logs and security camera tapes.

7b Policies and procedures for artifacts on long-term loan are re-iterated and disseminated concerning 1) the annual update of loan agreements and 2) requirements for long-term loans including photo requirements. LP should establish time caps on loans or periodically request temporary return of items for condition assessments.

7c Reiterate NARA policy to adequately backup inventory-related collection documentation.

8a Update comprehensive set of museum collection management policies and procedures and ensure their development.

8b Establish procedures to periodically review and, if necessary, revise said policies and procedures.

12-11 NARA's Network Assessment Audit

1 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

2 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

4 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

6 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

12 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

13 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

14 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

17 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

18 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

19 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

20 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

27 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

28 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

32 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

33 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

35 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

38 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

40 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

41 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

42 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

44 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

45 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

47 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

48 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

50 This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

12-15 Audit of NARA's Classified Systems

1 The Executive for Information Services/CIO (I), in coordination with the Chief Operating Officer (C), should ensure all classified system authorization packages are updated in accordance with NARA policy.

2 I, in coordination with C, should establish a timeframe for review and approval of authorization documents.

3 I, in coordination with C, should develop a continuous monitoring strategy for classified systems requiring system owners on at least a quarterly basis to assess security controls and inform authorizing officials when changes occur that may impact the security of the system.

4 I, in coordination with C, should obtain authorizations to operate for each of the classified systems or disallow them in accordance with NARA and Federal policy.

7a I, in coordination with C, should provide appointment letters for the SOs and ISSOs.

7c I, in coordination with C, should provide a sample of reading and record copies of signed appointment letters.

8 I, in coordination with C, should ensure all contingency plans are updated, completed, reviewed, and tested in accordance with NARA policy.

13-01 Audit of NARA's Internal Controls Program for FY 2010

1d Resources are employed to develop and implement the ICP including, but not limited to, a Chief Risk Officer, additional employees or contractors, and the purchase of appropriate ICP software.

1e Risk management responsibilities are included in the performance plans for program and function owners.

1f Prior recommendations from previous OIG and GAO reports are closed.

1g A Risk Management Policy is created to communicate NARA’s commitment to enterprise risk management.

1i A training plan is developed that encompasses educating the agency on risks and internal control. Additional training is provided to all individuals responsible for executing the ICP, including program owners, function owners, and MCOC members.

13-03 Audit of ERA Preservation Efforts

4 The CIO should conduct and document a thorough assessment of the production version of the ERA system's preservation framework capabilities.

13-08 Audit of NARA's Preservation Program (Textual)

1a The Archivist should ensure an overarching preservation strategy is developed. Additionally, a risk-based approach to holistically assess the agency’s preservation needs and design the agency's preservation plan should be implemented.

1b The Archivist should ensure an analysis is conducted of the organizational structure and responsibilities of each office involved in preservation. This should include a determination whether the preservation strategy can be effectively implemented with a decentralized structure, or if one NARA office should have authority over the entire Preservation Program.

2 The Chief Innovation Officer and Executives for Research Services and for Legislative Archives, Presidential Libraries and Museum Services, should ensure comprehensive preservation policies and procedures for each of their organizations are developed and/or updated.

3a The Chief Innovation Officer and Executives for Research Services and for Legislative Archives, Presidential Libraries and Museum Services should completely identify the resources necessary to adequately accomplish NARA's preservation mission.

3b Develop a plan to identify the complete universe of textual and non-textual records that require preservation.

4 The Executive for Research Services should ensure a detailed analysis is performed and communicate about the risks versus the benefits associated with not using the existing risk assessment data to calculate the backlog for the Washington area Archives.

5a The Executive for Research Services should ensure an analysis is performed to determine if additional risk assessments for the Washington area Archives and Presidential Libraries including older holdings should be completed. Identify the risks for not completing the assessments.

5b The Executive for Research Service should ensure additional measurable performance metrics are developed and implemented to track the progress within the Preservation Program.

5c The Executive for Research Services should ensure a cost benefit analysis for the HMS circulation Module is completed. Request required resources if the cost benefit analysis identifies benefits to the agency.

5d The Executive for Research Services should ensure Denver, St. Louis, and Special Media implement HMS to record risk assessments.

6 The Executive for Legislative Archives, Presidential Libraries and Museum Services should ensure an analysis is performed to identify whether HMS should be implemented across the Libraries. If it is decided HMS will be implemented, a timeline should be established. If it is decided HMS will not be implemented, identify (1) how the existing system will meet the agency's preservation needs and (2) obstacles and risks for not implementing HMS.

13-09 NARA's Data Backup Operations

2 The CIO should encrypt backup tapes containing sensitive PII or devise another method of protecting the data that provides a similar level of security.

4 The CIO should develop a process to regularly test data backups to verify information integrity.

10 The CIO, the Director of Acquisition Services, and NARA's Office of General Counsel should review purchases made for offsite storage costs to determine whether NARA's procurement process and Federal appropriations laws were violated and if so take appropriate corrective action.

13-10 NARA Archival Facilities

1a The COO should ensure a comprehensive review of the standards is completed. Additionally, roles and responsibilities for offices involved in the execution of the directive are clearly defined.

1b The COO should ensure a plan is developed including a timeline for when the archival storage facility reviews will be completed.

1c The COO should ensure an accurate listing of facilities currently compliant with the standards along with the area of deficiencies is identified and communicated.

1d The COO should ensure resources needed to make all archival storage facilities compliant by 2016 are identified. If the facility cannot be brought into conformance with the standards, determine and document what mitigating actions have been implemented.

1e The COO ensures PMRS is updated to accurately reflect percentage of archival holdings in appropriate space.

13-11 Audit of ERA Ingest Efforts

1 The COO assess Federal agency usage of Base ERA and implement a process to improve the records management workload and records management practices that exist between NARA and Federal agencies to ensure electronic records are being properly transferred.

2 The COO identify the most efficient and effective method of ingest and require Federal agencies to follow this method when transferring electronic records into base ERA. In addition this information should be properly disseminated to Federal agencies.

13-12 Audit of the NARA IDS

12 The CIO should ensure the preliminary reporting of all incidents and events reportable to US-CERT is made within the specified timeframes. Further details on the incident or event gathered after the original reporting should be communicated to US-Cert as an update.

14 The CIO should ensure incident response tabletop exercises are conducted for staff performing and/or supporting computer security incidents on at least an annual basis, and practical and relevant topics to NARA's computing environment are covered within the exercises.

15 The CIO should develop a policy for CIRT members to take training at least on an annual basis to ensure they remain up to date with current patterns/types of cyber attacks and effective, efficient incident remediation methodologies.

13-14 Audit of the Processing of Textual and Electronic Records

2b The Executive for Research Services should ensure the San Bruno, St. Louis, and Chicago field locations have a current processing backlog reduction plan. These plans should be developed yearly and updated periodically during the year as necessary.

2c The Executive for Research Services should ensure the cost-benefit analysis study on serving unprocessed records is completed, and that it outlines the risks and benefits of serving unprocessed records with an appropriate strategy consistent across the agency.

2d The Executive for Research Services should conduct a workload analysis to determine if resource allocation between the Washington and College Park facilities is appropriate.

3a The Executive for Legislative Archives, Presidential Libraries and Museums should analyze the backlogs at the pre-PRA libraries and create processing plans for reducing the backlogs at these libraries on a more accelerated basis.

3b The Executive for Legislative Archives, Presidential Libraries and Museums should assess if there are additional ways to accelerate processing at the PRA libraries.

4 The Executive for Research Services and the Executive for Legislative Archives, Presidential Libraries and Museums, should work with the Performance and Accountability Office to reassess current processing goals and make changes to the goals.

5a The Executive for Legislative Archives, Presidential Libraries and Museums should work with the Performance and Accountability Office to develop a performance measure for tracking the process of electronic presidential records.

5b Determine the true backlog of electronic presidential records and determine if additional resources are needed and can be obtained to handle the increased workload.

6 The Executive for Legislative Archives, Presidential Libraries and Museums and the Executive for Research Services should ensure a review is performed to validate the accuracy of processing data supplied to the Performance and Accountability Office.

7 The Executive for Research Services should ensure procedures for all field locations are documented. Review existing procedures and update as necessary.

8 The Executive for Legislative Archives, Presidential Libraries and Museums should ensure procedures for all Presidential libraries are documented, and review existing procedures and update them as necessary.

14-01 Oversight of NARA's Energy Savings Performance Contracts (ESPCs)

8 NARA should establish formal assessment criteria and future savings analysis for use in determining whether to cancel ESPCs.

14-04 Audit of the Use of Presidential Libraries by Outside Organizations

4 Presidential libraries should work with NARA's general counsel to institute general counsel review program of a sample of applications for use (16011 forms) from all Presidential libraries to ensure the forms meet the requirements of 36 CFR 1280.94.

5 We recommend all Presidential libraries create and maintain rental guidelines that help to ensure compliance with 36 CFR 1280.94.

14-05 Audit of NARA's Field Offices Acquisition Activity

1a NARA should establish and implement a tracking system to document and monitor training for all contracting officers ensuring compliance with the Federal Acquisition Certification in Contracting policy memorandum.

1b NARA should consider terminating field office contracting officers' warrants until all initial training requirements are met.

2 NARA should ensure all field office contracting officers and buyers are adequately trained on how and when to close out NARA contracts. Additionally, periodic monitoring and testing of closeout procedures should be conducted to ensure contracts are closed out in a timely manner.

3 NARA should establish and implement a formal documented process for informing the field office support team of field office contracts requiring review prior to award.

4 Update NARA policies to ensure the guidance for approval of small and small disadvantaged business utilization exceptions is consistent.

14-07 Audit of NARA's Payments to Federal Agencies (excluding GSA)

4 Update NARA Interim Guidance 402010, Reimbursable Work Authorizations and Security Work Authorizations to provide guidance on what controls are needed over procurement vehicles, such as an SWA covering multiple events, and what supporting documentation is needed.

14-08 Audit of NARA's Capital Planning and Investment Control (CPIC) Process

1a The CIO should ensure any changes to NARA's CPIC policy are promulgated in the form of a NARA notice and published on the NARA@Work Intranet site.

1b The CIO should ensure all required CPIC related documentation is completed for all NARA IT investments going through the CPIC process.

1c The CIO should require the creation and use of a checklist outlining the IT governance related documentation required to be completed for all IT investments going through the CPIC process.

2 The CIO should require NARA's updated CPIC policies and procedures meet the CPIC process requirements detailed in the Clinger Cohen Act.

3 The Chief Operating Officer (COO) should ensure NARA IT investments do not bypass NARA's CPIC process.

5 The COO should ensure I-P maintains documentation of its approval of IT investments in PRISM and I-P's PRISM approval of IT investments is tested on an annual basis with all documentation of this testing sent to NARA's internal controls group.

6 The COO should ensure the training guide for purchase card holders is updated to include a discussion of the requirements of NARA's CPIC Process.

7 The CIO should distribute a NARA Notice annually to remind employees of their CPIC responsibilities related to the acquisition of IT investments.

8 The CIO should ensure NARA's IT governance process, which includes CPIC, incorporates the lessons learned when Directive 801 was followed to create a more user-friendly, streamlined, and transparent policy where CPIC requirements align closely with the costs of IT investments.

9 The COO should consider including an enforcement mechanism in any updates to NARA's CPIC policy.

14-09 Audit of Conference-Related Activities and Expenses

2a The CFO should ensure communication is provided to offices regarding adherence to conference policies, including penalties for non-compliance.

2b The CFO should ensure interim guidance 165-1, Conference-Related Activities and Expenses, is updated to incorporate statutory requirements for reporting to the OIG any conferences where expenses exceed $20,000.

2c The CFO should ensure methodology is developed for gathering and reporting post-conference details, including details of all expenses and justification when total costs increase by a threshold established by management. This should include a time frame for reporting.

14-10 Audit of NARA's Enterprise Wireless Access

1d NARA should assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements.

1e NARA should authorize network operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable.

1f NARA should monitor the security controls in the network on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analysis of the associated changes, and reporting the security state of the system to designated officials.

2c This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

2g This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

3 NARA should develop, document, review, update, and implement wireless policies and procedures on at least an annual basis in accordance with internal NARA and NIST requirements.

4a NARA should utilize existing WLC and WAP baseline configurations or develop its own baseline configurations.

4b NARA should implement a process to monitor the WLC and WAP settings for compliance with the established baseline configurations.

4c NARA should document and approve any deviations from the WLC and WAP baseline configurations.

4d NARA should maintain older versions of the baseline configurations as necessary.

5a NARA should implement a process to conduct vulnerability scans that identify weaknesses related to NARA's wireless environment.

5b NARA should develop procedures to analyze and remediate the vulnerabilities identified.

14-11 Audit of Special Telework Arrangements at NARA

1 The Chief Human Capital Officer (CHCO) should develop controls and relevant control activities to ensure telework agreements are in place, reviewed, and renewed by the employee and the supervisor annually, and a copy of the approved, disapproved, or terminated telework agreement is provided to the NARA Telework Managing Officer.

2 The CHCO should provide clarifying guidance to supervisors as to which arrangements require executive or staff director approval.

3 The CHCO should establish an oversight mechanism to ensure employees’ duty station assignments are reviewed and validated periodically.

4 The CHCO should seek reimbursement of the $4,447 overpayment or grant a waiver in accordance with 5 U.S.C. 5584.

5 The CHCO should issue additional guidance for long-distance telework arrangements to require supervisors to conduct a cost/benefit analysis of the proposed arrangement and document this analysis. For those arrangements resulting in additional costs to NARA, supervisors should be required to justify how the arrangement is in the best interest of NARA.

8 The CHCO should revise the Telework Agreement (form 3040) or issue additional guidance for full-time and long-distance telework to require supervisors and employees to estimate the time frame for the arrangement, while still subject to the annual renewal.

9 The CHCO should revise NARA 332 to include a requirement that new telework agreements be prepared and signed when a new employee/supervisory relationship is established.

11 The CHCO should communicate best practices for monitoring telework employees and best practices in establishing special telework arrangements across the agency.

14-12 Audit of Selected Aspects of NARA's Digitization Program

4 The Chief Innovation Officer should track and report progress on each of NARA's digitization strategies.

9 The Chief Innovation Officer should develop a reporting methodology that tracks total traditional records made available through NARA's public access system.

10 The Chief Innovation Officer should distinguish in reporting what quantity of records is available online through NARA, and what quantity is accessible online through partnership websites.

11 The Chief Innovation Officer should ensure future Annual Performance Plans accurately reflect current data regarding traditional records availability.

15-01 Audit of FISMA for FY 2013

1 Develop new policies and procedures or update existing policies and procedures for at least the 11 programs areas included in the annual FISMA review.

2 Coordinate with the Office of Performance and Accountability and NARA's Chief Risk Officer to identify, assess, capture, and report IT Security controls within NARA's Internal Control Program Tool in order to adequately ensure safeguarding of assets.

15-02 Audit of NARA Mobile Security

1a Develop and document a strong internal control process for ordering, activating, and deactivating mobile devices and phone lines to ensure no unnecessary phone lines exist and incur costs.

1b Develop and document a strong internal control process for reviewing monthly bills for items including user names, activities, plan adequacy, and opportunity for cost savings.

1c Develop and document a strong internal control process for determining when an additional charge will be considered for reimbursement.

2 Review and update NARA's current policy documents for use of NARA-issued mobile devices, including NARA 813-1 and NARA 802 to reflect more complete and accurate information an acceptable uses of the devices and when a disciplinary action will be requested.

3 Provide training to educate users on acceptable uses of NARA-issued mobile devices, including requesting a travel device for international travel.

4 Develop a formal policy for interaction of NARA-issued mobile devices with other systems and update NARA 813-1 to clearly reflect the policy.

6 Re-evaluate the current lockout settings to better protect the data from unintended disclosure and/or misuse.

7a Develop a comprehensive lost mobile device control process to include all lost or stolen mobile devices are managed on a centralized list with detailed information such as user's name, phone number, date lost/stolen and found, and status.

7b Develop a comprehensive lost/stolen mobile device control process to include the Remedy incident management system and ensure any task requiring contractor effort is appropriately communicated to ensure that data on all list of stolen devices is safeguarded.

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

8b Develop and document policies and procedures on mobile device retirement management process, defining the steps needed to be performed, by responsible party for each step, and the monitoring and reporting process.

15-03 Audit of Specially Protected Records

1 Ensure NARA 1572 is updated to require custodial units to report their storage methods and exact containers locations and names of staff members and the specific areas to which they have access to BX.

2a Security Management performs initial certifications of Specially Protected Holdings (SPHs) storage areas.

2b Security Management performs security inspections of SPHs storage areas.

2c Security Management develops guidelines for SPHs security inspections, including timeframes, criteria, documenting requirements, and reporting requirements.

3 Ensure an analysis is performed to determine if staff with access to SPHs, positions should be designated higher than low risk positions. Based on the analysis, nominate selected staff for required background investigations.

4 Ensure Security Management maintains copies or obtains access to SPHs inventory listings and use them to randomly select records and verify their condition and location during inspections.

5a SPHs inventory listings are completed at the item level. Establish a timeframe for when the listings must be completed. Communicate with other offices to identify best practices used in documenting their inventories.

5b Inventory listings are reviewed to determine their accuracy and update as necessary.

5c A finding aid is created for the agency's entire SPHs collection at the item level.

5d Locked hard copies of the inventory listings are maintained.

5e SPHs inventory listings are maintained in the Holdings Management System (HMS). All electronic versions of the listings are password protected and access limited to authorized employees.

6 Ensure NARA 1572 is updated to include (1) responsibilities for Security Management to review annual inspections, including documenting the review, for compliance with NARA 1572, (2) timeframes for when Presidential Libraries and Field Office Archives should complete annual inspections, and (3) the amended requirement for annual inspection reports to include the date of the inspection, individuals that complete the inspections, and a listing of items inspected, including their location and physical condition.

7 Ensure all Presidential Libraries are in compliance with NARA 1572 policy of conducting annual inspections.

8a Initial inspections of SPHs inventory are completed.

8b Custodial units are in compliance with NARA 1572, including randomly inspecting at least three percent of SPHs inventory annually on a rotating basis and using one individual that does not work for the individual responsible for the inspection.

8c Annual inspection reports include at a minimum date of inspection, individuals who complete the inspections, and a listing of items inspected, including their location and physical condition.

8d Annual inspection results are adequately documented and communicated to Security Management and office heads.

9a Staff is properly trained and retained to use charge out cards whenever records are removed from SPHs storage areas.

9b Access to SPHs storage areas is properly monitored, including keeping the list of those persons with access to the SPHs areas updated at all times and restricting access to only authorized staff.

10a Required elements for the handling of SPHs for each record storage area should be communicated to each custodial unit.

10b Detailed procedures are documented for each custodial unit.

10c A process is in place for periodic review of procedures and updates are made as needed.

15-06 Audit of the Processing of Military Interfiles and Refiles at the National Personnel Records Center

1 Ensure an analysis is performed to determine whether the five percent interfile batch reviews are reasonable and update NPRC 1865.126 if needed.

2a Ensure standards are outlined for how the batch control application (BCA) will select interfile documents for all reviews, including after defects are identified.

2b Ensure the BCA is configured to (1) accurately capture all reviews performed; (2) accurately select the documents for interfile reviews based on the agreed percentage including any additional reviews; and (3) identify documents selected for reviews.

2c Periodic BCA reports are created and reviewed to evaluate the interfile review process.

3 Ensure supervisory controls are put in place for the interfile and refile processes, including items to be reviewed, timing, and evidence of the reviews.

15-10 Audit of Digitization Partnership Process

1 Conduct an agency-wide inventory of Digitization Partnerships and update NARA's partnership webpage to reflect current partners.

2 Establish criteria for which Digitization Partnerships require public notification and approval by the Archivist of the United States.

4 Develop criteria for partners starting new projects while others are incomplete or on hold for prolonged periods of time.

5 Establish procedures to review partnership image and metadata for proper formats at the time of digitization.

7 Work with NARA Executives to determine what staffing resources are needed and available to most effectively leverage NARA's Digitization Partnerships.

8 Establish a process that ensures NARA's Digitization Partnership Strategy, Principles for Partnerships, and digitization policy are reviewed and updated on a regular and timely basis.

15-11 Audit of Digitization Storage

1 Develop a long-term strategy for internal digitization infrastructure needs and periodic technical refreshes of equipment used in the Digitization Labs.

2 Develop procedures for file management of digitized records in the Digitization Labs and develop contingency plans for staff charged with managing the infrastructure of the Digitization Labs.

3 Implement a central file repository system in the Digitization Labs.

4 Develop agency-wide policies and procedures for digital file preservation.

5 Implement increased storage solutions for digitization efforts at the Presidential Libraries.

6 Develop a long-term strategy for increasing transfer capabilities between various internal storage systems housing digitized records.

7 Develop a long-term storage strategy for currently held partner data and partner data to be provided to NARA in the future.

8 Work with partners to return partner-provided hard drives,

9 Establish procedures for the transfer of digitized records received from NARA's Digitization Partners to NARA and the handling of those records once in NARA's possession.

13 Perform an analysis of the 350 million records offered to NARA by one partner to determine what records NARA should take possession.

15-13 Audit of HR systems and data Accuracy

1 Fully implement the new supervisor information update process in FPPS and conduct a review of the information on a periodic basis to ensure the information remains accurate and complete.

4a Create an Employee Locator update policy including the following a defined timeframe within which employees are required to review and update Employee Locator entries.

4b Create an Employee Locator update policy including the following supervisors' responsibility to ensure employee contact information remains complete and accurate

5 Include in the new hire orientation the requirement to update Employee Locator entries, based on the policy created from recommendation three.

8 Consider developing and providing user training on populating reports in Datamart, and providing managers and supervisors with permission to populate reports for their office or the employees they supervise.

9a Ensure user accounts for separated employees are removed timely.

9b Ensure roles and privileges assigned to the users are commensurate with their current job responsibilities.

10 Re-evaluate the option to utilize eCStaffing to manage personnel data for non-federal workforce at NARA and use the HRMS as the single authoritative data source for the HSPD-12 LACS implementation.

11 Establish on authoritative data source that provides the latest data to role-based users on NARA's federal employees, contractors, and volunteers at the enterprise level.

15-14 Audit of Space Management for Paper Records

1 Consider implementing records management guidance to make agencies report to NARA records in their possession 30 years or older on a more regular basis.

2 Implement a strategy to work with other federal agencies to resolve "limbo" records and schedule those records for accessioning or disposal.

3 Work with R to facilitate consistent application of HMS at all archival facilities, to capture all archival holdings in HMS, and improve how HMS calculates the available space.

4 Establish a permanent group to both track and manage space and advise NARA management on space matters across the agency.

5 Develop a long-term space management strategy for the agency.

6 Develop cost estimates for potential solutions.

7 Incorporate space management into NARA's strategic planning initiatives and include the agency's space need in all necessary reporting. Considering reporting space management as a Material Weaknesses and track it appropriately

8 Create a timeline for the agency to have necessary discussions with both internal and external stakeholders to address NARA's space challenges.

9 Develop requirements necessary for NARA to prepare a budget request to address the agency's critical space challenges. After a strategy is implemented and requirements are developed, prepare and submit a budget request.

15-15 Cabling Audit

1 NARA incorporate all locations into the NARANet SA&A package by documenting location-specific security controls and ensuring that they are appropriately tested and monitored.

2.1 Ensure that neat cable management and labeling mechanisms are employed for all sites.

2.2 Ensure that all server rooms are equipped with appropriate fire detection and suppression capabilities.

2.3 Limit access to all server rooms to those individuals with an explicit need to access IT equipment.

2.4 Ensure that appropriate temperature and humidity monitoring and control mechanisms are employed for all server rooms.

2.5 Ensure that appropriate UPS devices are employed for hardware supporting the site's network infrastructure.

2.6 Ensure that all server racks, switches, and network equipment are adequately secured from unauthorized access via locked racks.

3 NARA develop and implement a plan to install additional networking capabilities at facilities that are near capacity, or develop and implement a contingency plan to support continued operations in the event that networking capabilities are maximized.