OFFICE *of* INSPECTOR GENERAL

SEMIANNUAL REPORT *to* CONGRESS

APRIL 1, 2016 *to* SEPTEMBER 30, 2016

FOREWORD

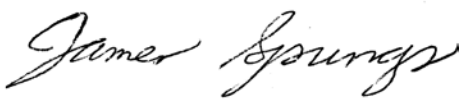
I am pleased to present this Semiannual Report to Congress covering the oversight activities of the Office of Inspector General (OIG) for the National Archives and Records Administration (NARA) from April 1, 2016, to September 30, 2016. Our products continue to assess the effectiveness, efficiency, economy, and integrity of NARA's programs and operations.

During this period the OIG spent a considerable amount of time educating the agency on the role and responsibilities of the OIG, and discussing tenets of the IG Act. It is critical for all NARA personnel to understand the OIG is an independent unit within NARA charged with detecting and preventing fraud, waste, abuse, and mismanagement. Through our audits, investigations, and other inquires we help the agency run its programs and operations more effectively and efficiently. Essential to our independence is the fact that management may not prevent or prohibit the OIG from initiating, carrying out, or completing its work.

We held our first open house at NARA's facility in College Park, MD to help educate people on the mission and activities of the OIG. While our intent was merely to provide information, we learned an unfair labor practice was filed against NARA over the open house, as the appropriate union was not given specific notification. We hope to hold open houses at multiple facilities in the future, and have instituted a procedure to ensure proper notifications go out. In addition, we gave outreach briefings to NARA personnel at regional and library facilities across the country, and new employee orientation presentations in the National Capital area. We also continued running the Whistleblower Ombudsman Program, providing training and information to potential whistleblowers on various rules and protections available. This work included updating the OIG website, one-on-one consultations with employees, meeting with the Senate Whistleblower Caucus, and providing training to NARA employees.

These educational efforts foster better understanding and communication, effect positive change and outcomes, and reduce the likelihood of incidences such as the one that occurred this period. Specifically, NARA refused to allow the OIG independent access to employee emails to review them for potential violations of the Hatch Act. In management's opinion, the OIG should not be allowed "unfettered" access to NARA information, and management should be allowed to act as a gatekeeper to control the flow of information to the OIG. When the OIG requested access to all NARA emails to run computer searches on them, NARA refused. Management stated the OIG should only search for violations "based on information that a specific person or persons are engaged in misconduct." However, at a subsequent meeting NARA offered to run the searches if the OIG provided search terms, and NARA would provide the OIG with the results. While in the end NARA provided the information sought, we believe based upon the IG Act it was impermissible for the agency to actively interject itself into an OIG review and become the arbiter of if, or how, the OIG has access to NARA information.

I continue to be extremely 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 its audit and investigative efforts.



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 56th Semiannual Report to Congress summarizing the activities and accomplishments of the National Archives and Records Administration (NARA) Office of Inspector General (OIG).

Audits and Reports

The OIG 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 OIG issued the following audits and other non-audit reports, including a management letter. Each report portrays a snapshot in time at the end of the fieldwork, and may not reflect the current situation at the end of the reporting period.

Audits of Programs and Operations

- **Reissued Audit of NARA's Preparation and Planning for the Receipt of President Obama's Administration's Records and Artifacts –** NARA had implemented internal controls related to textual records, classified records, and the artifacts/gifts in NARA's courtesy storage. These appeared to be operating effectively. Although NARA was addressing technical aspects and working with the Executive Office of the President (EOP) to prepare for the transition of electronic records to NARA's physical custody, NARA lacked assurance the Electronic Records Archive (ERA) EOP system will respond as intended to a significant ingest. NARA had not received a comprehensive inventory, or a large volume of electronic records to adequately test the system. As a result, NARA may not be able to rely on the ERA EOP System to comply with the Presidential Records Act and respond to special access requests in a timely manner. In addition, NARA lacked a documented contingency plan. NARA officials were confident, based on planning and analyses, that the ERA EOP System will be able to adequately handle electronic records from the Obama administration. However, NARA had no control over the quality of the data samples or when the data will be transferred. Without a contingency plan in place, NARA lacked assurance that it will be able to rely on the ERA EOP. (OIG Audit Report No. 16-06, dated May 6, 2016. See page 12.)

- **Audit of NARA's Refile Processes at Selected FRCs –** NARA Federal Records Centers (FRCs) did not meet required timeframes for refiling IRS records and did not accurately report the refile backlog times. Additionally there were no inventory listings to track records received; records were refiled incorrectly; and there was no process to track problems and resolutions at the FRCs. Inconsistent processes were also found for quality control; verifying refile batch volumes; numbering batches; and tracking IRS record locations within the FRCs. We attribute these conditions to the need for standardized policies and procedures for IRS records at the FRCs. The lack of a coordinated approach for the IRS records limits the FRCs' ability to collectively meet the requirements of the interagency agreement between NARA and the IRS. (OIG Audit Report #16-07, dated May 17, 2016. See page 13.)

- **Audit of NARA's FY 2015 Compliance with Improper Payment Requirements**
  NARA's programs and activities were compliant with improper payment requirements. Specifically, NARA was fully compliant with requirements to publish a report and conduct program-specific risk assessments. Based on risk assessments for each program or activity, NARA determined they were not susceptible to significant improper payments and therefore were not required to perform four of six requirements. However, NARA's reporting did not satisfy all the requirements of OMB Circular A-136, Financial Reporting Requirements. (OIG Audit Report #16-08, dated May 26, 2016. See page 13.)

Other Reports Concerning NARA Programs and Operations

- **Second Evaluation under the Reducing Over-Classification Act**
  The Information Security Oversight Office (ISOO) at NARA develops government-wide security classification policies and evaluates the effectiveness of the security classification programs at Federal agencies. ISSO's Director has the responsibility to make classification determinations when there is an exceptional need to classify information, but an agency with appropriate subject matter interest and classification authority cannot be readily determined. ISOO's Director has never used this authority, but would follow the appropriate policies and guidance, if needed. (OIG Report CR-16-1, dated May 12, 2016. See page 14.)

- **NARA's Compliance with the Cybersecurity Information Sharing Act of 2015**
  The Cybersecurity Information Sharing Act of 2015 requires OIGs to report on their agencies' covered systems. "Covered systems" are defined as national security systems, or Federal computer systems providing access to personally identifiable information (PII). NARA has policies and procedures in place for logical access controls including multifactor authentication for privileged users to access covered systems, and data security management practices for NARA and other entities (including contractors). However, NARA has not implemented and followed its process and procedures for some covered systems. Eighteen of thirty NARA identified covered systems do not have multifactor authentication implemented for privileged users. NARA indicates many of these 18 systems are either not connected to the network, or hosted by a third-party. These systems require privileged users to access the covered system with a username and password. However, NARA's own IT Security Requirements document states users with elevated security privileges shall access the system using a multi-factor authentication mechanism that complies with applicable Federal directives and NARA policy. The 18 covered systems are not in compliance with NARA policy. (OIG Report CR-16-2 dated August 11, 2016. 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 offering insight on how to correct them.

In this period the OI received and reviewed 252 complaints and other intake actions, opened 13 new investigations, and closed 17 existing investigations. Four matters presented for potential criminal prosecution were declined. During this period the OI initiated a new kind of investigative review, an "assessment," proactively looking into aspects of NARA's programs and operations such as contract compliance and telework adherence.

For fiscal year 2016 as a whole:

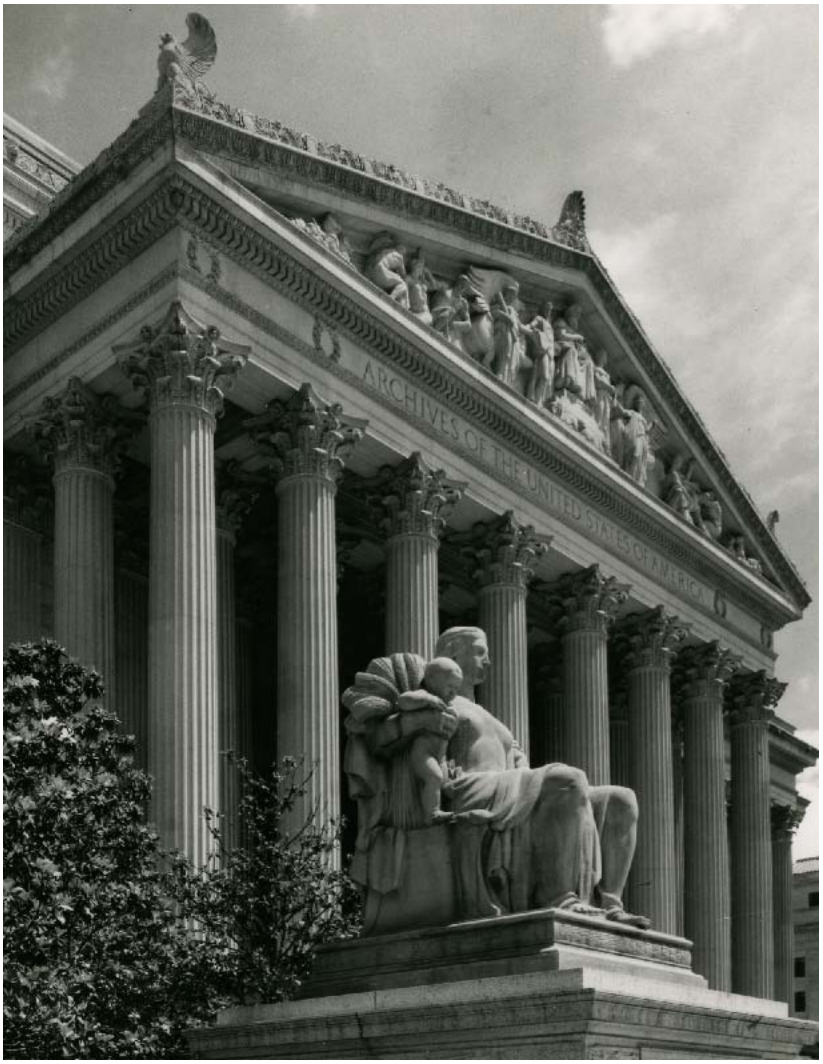
- Ninety percent of our closed investigations resulted in referrals for criminal, civil, and/or administrative action.
- OI special agents made 14 outreach briefings to over 300 NARA employees all across the country, and 15 new employee orientation presentations to 110 new employees in the National Capital area.
- Approximately 25 percent of the investigative matters reviewed involved allegations of inappropriate use of Information Technology resources. Clarified policy, better monitoring, and the deterrence effect of successful disciplinary action are hoped to result in significant cost savings and productivity in the coming year.

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.

- Held a public OIG Open House at the NARA facility in College Park, MD to help educate people on the mission and activities of the OIG. This was the first Open House, and the OIG hopes to have these events at multiple facilities in the future.
- Worked with the agency to review proposed changes to Privacy Act systems of records notices.
- Continued running the Whistleblower Ombudsman program, providing training and information to potential whistleblowers on various rules and protections available. This work included updating the OIG website, one-on-one consultations with individuals, meeting with the Senate Whistleblower Caucus, and providing training.

- Responded or worked on multiple requests for OIG records under the Freedom of Information Act (FOIA), including large scale requests for large amounts of records relating to various criminal investigations.
- Worked with agency counsel to ensure the OIG's independence and authority was accurately reflected in a revised directive on the agency's alternative dispute resolution program.
- Provided comment and input into several other NARA directives and regulations covering a variety of topics.
- Coordinated with agency general counsel to ensure the OIG was covered by NARA's whistleblower compliance certification to the Office of Special Counsel.
- Worked with NARA IT employees working with OIG systems or providing IT assistance to ensure relevant individuals had signed confidentiality/non-disclosure agreements in place.
- Responded to over 40 requests from NARA for reviews of proposed legislation, Office of Management and Budget (OMB) regulations, Congressional testimony, and other items.
- Began developing an office specific OIG logo with NARA design professionals.



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 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 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 Record 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 2016, NARA had 100 million online visits in addition to hosting 3.5 million traditional museum visitors, all while responding to more than 1.3 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 2,907 full-time equivalents (FTEs), NARA operates 44 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 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's appropriation, including authorization for 24 FTEs. During this period the Assistant Inspector General for Audits (AIGA) and Assistant Inspector General for Investigations (AIGI) positions were approved by the Office of Personnel Management to be Senior Executive Service (SES) positions, and the Counsel to the IG was approved to become a Senior Level position. At the close of the period applicants for the AIGA and AIGI positions at the SES level were being evaluated. Sadly, the longtime Administrative Assistant at the OIG departed the office for another position this period. At the close of the period the office had begun the search for their replacement. Currently the OIG has 18 FTEs on board, including an Inspector General, nine 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. Counsel remains involved in various aspects of the Committee's work including assisting in creating a draft views letters; answering various data calls; monitoring legislation for developments of interest to the community; and developing input for proposed legislative actions.

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.

Inspector General Training

The OIG counsel continued to work with the CIGIE Training Institute teaching the Inspector General Authorities course. Counsel also assisted the IG Academy at the Federal Law Enforcement Training Center, instructing criminal investigators on various legal topics.

Whistleblower Ombudsman Working Group (WOWG)

In accordance with the spirit of the Whistleblower Protection Enhancement Act of 2013, the IG appointed the OIG counsel as the whistleblower ombudsman. Counsel meets with the WOWG to develop best practices, discuss community-wide issues, and learn about training programs.

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 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 have fully implemented all recommendations, as the last two outstanding recommendations were implemented on October 1, 2016.

NARA OIG Peer Review of the Securities and Exchange Commission OIG

As previously reported, the 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

As previously reported, 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 Congress informed about agency and OIG activities, the OIG responded to the following items:

OIG Survey on Criminal Referrals

The OIG responded to a survey from the Committee on Oversight and Government Reform asking for information on criminal referrals made by the OIG. In FY 2015 the OIG made eight referrals, six concerning NARA employees, one concerning a NARA contractor, and one concerning a private citizen.

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 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.

NARA Research Room Complaint

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

Audit and Reports Overview

During this reporting period, the OIG issued three final audits, and two other major reports. The information below is based on results at the conclusion of field work, as depicted in the final reports. It is possible that NARA may have made improvements and/or addressed some of the issues after such time. We initiated or continued work on audits or other non-audit 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 Enterprise-wide Risk Assessment of internal controls and associated risks to NARA's mission, operations, and procedures (this work has been contracted out to an independent private auditor);
- NARA's Management Control over Microsoft Access Applications and Databases, identifying the MS Access applications/databases in use; assessing security controls; and determining whether NARA is appropriately positioned to accommodate and maintain the applications and associated databases;
- NARA's Compliance with Federal Managers Financial Integrity Act (FMFIA) for FY15, 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 operated or maintained; and whether all NARA systems have been classified and categorized as required;
- Consolidated Audit of NARA's FY 16 Consolidated Balance Sheets as of September 30, 2016 and the related Statements of Net Cost, Changes in Net Position, and Budgetary Resources (this work has been contracted out to an independent private auditor);
- Evaluation of NARA's Compliance with the Federal Information Security Modernization Act (FISMA);
- NARA's Cloud Computing Efforts, evaluating NARA's cloud computing environment to determine whether NARA is properly prepared to manage its transition to cloud computing services and meet OMB's goals of a "Cloud First" policy;
- NARA's Electronic Records Archives (ERA) System, evaluating and reporting on the current status of the ERA 2.0 development effort; and
- NARA's Freedom of Information Act (FOIA) Process, determining whether NARA's FOIA process is efficient, effective, and complies with current laws and regulations.

Audit Summaries

NARA's Preparation and Planning for the Receipt of President Obama's Administration's Records and Artifacts

On January 20, 2017, legal custody of the records from President Barack Obama's administration will transfer to the National Archives and Records Administration (NARA). The Presidential Records Act (PRA) gives the Archivist of the United States (AOTUS) responsibility for the custody, control, and preservation of Presidential records upon the conclusion of a President's term of office. The PRA states the AOTUS has an affirmative duty to make such records available to the public as rapidly and completely as possible, consistent with the provisions of the Act. However, such public access does not commence until five years after the President leaves office. In addition, NARA strives to be able to respond as soon as possible to time-sensitive and often high-visibility special access requests for these records, which come from former and incumbent Presidents, the courts, and Congress. Providing such access, however, must be consistent with the Archivist's responsibility for assuming "the custody, control, and preservation of" the Presidential records.

The objective of this audit was to review the preparation and planning for the transfer of the Obama Administration's records. Specifically, we reviewed planning for the receipt of textual and electronic records, as well as artifacts/gifts from the Obama Administration. We found internal controls related to textual and classified records; and the artifacts/gifts in courtesy storage, had been implemented, and appeared to be operating effectively.

We also found, although NARA was addressing the technical aspects of the transfer and working with the staff of the Executive Office of the President (EOP) to prepare for the transition of electronic records to NARA's physical custody, NARA lacked assurance the Electronic Records Archive (ERA) EOP system will respond as intended to a significant ingest. NARA had not received a comprehensive inventory, or a large volume, of electronic records from the current administration to adequately test the ERA EOP system. As a result, NARA may not be able to rely on the ERA EOP System to comply with the PRA and respond to special access requests in a timely manner.

In addition, NARA lacked a documented contingency plan should the ERA EOP System fail to handle the Obama electronic records in a timely manner. Based on the planning and analyses performed, NARA officials were confident the ERA EOP System will be able to adequately handle the electronic records from the Obama administration. However, NARA had no control over the quality of the data samples or when the data will be transferred. Without a contingency plan in place, NARA lacked assurance it will be able to rely on the ERA EOP System to comply with the PRA. While we recognized that many of these issues are outside of NARA's control, and the administration is not required to provide any records to NARA prior to inauguration day, this does not relieve NARA of its responsibilities under the PRA.

This report was re-issued because management sent a revised response to the OIG ten days after the final report was originally issued. Management added a statement in their revised response that acknowledged this report, as with all audit reports, only addressed matters up to the

conclusion of audit field work, and reiterated field work ended in January 2016, as is stated on page seven of the report.

We made two recommendations to enhance NARA's preparation for the electronic records from President Barack Obama's administration and its compliance with the PRA.

NARA's Refile Processes at Selected Federal Records Centers

NARA's Federal Records Centers (FRCs) store records for agencies, including individual and corporate tax returns for the Internal Revenue Service (IRS). Under an interagency agreement between NARA and the IRS, NARA provides for the retirement and storage of tax records, reference services, refiles, interfiles, taxpayer photocopy, relocation of documents, and any mandated security upgrades. At the request of the Archivist of the United States, the Office of Inspector General (OIG) conducted an audit of NARA's refile processes of IRS records. The audit assessed the effectiveness and adequacy of management controls in place for refiles of IRS records at several FRCs.

We identified weaknesses related to the timeliness, reporting, and accuracy of IRS refiles. Specifically, FRCs visited did not adhere to the timeframe requirements for refiling of IRS records as specified in the interagency agreement and did not accurately report the refile backlog times. Additionally, there were no inventory listings to track records received; records were refiled incorrectly; and there was no process to track problems and resolutions at the FRCs.

There were also inconsistent processes for quality control, verifying refile batch volumes, numbering batches, and tracking IRS record locations within the FRCs. We attribute these conditions to the Federal Records Centers Program (FRCP) Operations' need for standardized policies and procedures for IRS records at the FRCs. The lack of a coordinated approach for the IRS records limits the FRCs' ability to collectively meet the requirements of the interagency agreement between NARA and the IRS. Additionally, NARA could be at risk of losing a key funding source, which is essential for FRCs.

This report makes fourteen recommendations to initiate improvements which, when implemented, should help strengthen FRCs' refile processes for IRS records.

Audit of NARA's FY 2015 Compliance with Improper Payment Requirements

The Improper Payments Information Act of 2002 (IPIA; Public Law (P. L.) 107-300), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA; P. L. 111-204), and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA; P. L. 112-248), requires agencies to annually report information on improper payments to the President and Congress through their annual Performance and Accountability Reports (PAR) or Agency Financial Reports (AFR).

The objective of this audit was to determine NARA's compliance with improper payment requirements based on Office of Management and Budget (OMB) Memorandum 15-02 and OMB

Circular A-136. Per IPERA, if an agency does not meet one or more of six requirements, the agency is not compliant.

We found NARA's programs and activities were compliant with improper payment requirements. Specifically, NARA was fully compliant with IPERA requirements to publish a PAR or AFR (completed on November 16, 2015) and conduct program specific risk assessments (completed in FY 2014).

Based on risk assessments for each program or activity (Administrative Overhead, Agency Services, Electronic Records Archives, National Historical Publications and Records Commission, Legislative Archives, Presidential Libraries and Museum Services, Repairs and Restoration and Research Services), NARA determined the programs and activities were not susceptible to significant improper payments and therefore were not required to perform four of six requirements. However, NARA's reporting on IPERA was not complete and did not satisfy all reporting requirements in OMB Circular A-136, Financial Reporting Requirements.

This report makes one recommendation to improve NARA's reporting on improper payments in the Agency Financial Report.

Summaries of Other Major Reports

Second Evaluation under Public Law 111-258, the Reducing Over-Classification Act

Public Law 111-258, Section 6(b) mandates Inspectors General of Federal departments, or agencies with an officer or employee who is authorized to make original classifications, shall carry out no less than two evaluations to: (A) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and (B) identify policies, procedures, rules, regulations or management practices that may be contributing to persistent misclassification of material. The initial evaluation was to be completed no later than September 30, 2013 and the second evaluation by September 30, 2016. The second evaluation is to review progress made pursuant to the results of the first evaluation.

Our initial evaluation entitled *Evaluation under Public Law 111-258, the Reducing Over-Classification Act* was issued on September 20, 2013 and disclosed NARA does not have original classification authority. However, the Director of the Information Security Oversight Office (ISOO) was designated with original classification authority by the Presidential Order, "Original Classification Authority," (OCA), dated December 29, 2009. ISOO, an administrative component of NARA, is responsible to the President for policy oversight of the Government-wide security classification system and the National Industrial Security Program. The Director of ISOO has responsibility for classification determinations in instances when there is an exceptional need to classify information but an agency with appropriate subject matter interest and classification authority cannot be readily determined. The Director of ISOO has never used this authority.

The Director of ISOO does not have a classification guide due to the lack of instances of this type of special classification. In addition, the ISOO develops security classification policies for the Government and evaluates the effectiveness of the security classification programs

established by Federal agencies. The Director of ISOO would follow the policies found in Executive Order 13526, Part 1 and 32 CFR, Part 2001, Subparts B and C guidance, if needed.

Since the initial assessment determined the Director of ISOO was designated with original classification authority, but never used it, our second assessment determined if this authority was used after the completion of our initial assessment. We contacted the Acting Director of ISOO, who confirmed that neither he nor the prior Director used original classification authority. In addition, he stated the information in our initial evaluation is still accurate.

NARA's Compliance with the Cybersecurity Information Sharing Act of 2015

The Cybersecurity Information Sharing Act of 2015 (Cybersecurity Act) requires Inspectors General of covered agencies submit a report on their agencies' covered systems. "Covered agencies" are those operating "covered systems;" defined as national security systems, or Federal computer systems providing access to personally identifiable information (PII).

We requested a list of the National Archives and Records Administration's (NARA's) covered systems, as well as documentation for each covered system related to the information security management practices outlined in the Cybersecurity Act. NARA identified 30 systems meeting the definition of a covered system, including 9 national security systems and 21 systems providing access to PII. NARA also provided responses to the specific questions in the Cybersecurity Act. We evaluated whether logical access policies and practices were followed. We did not independently verify, analyze, or validate the list provided. However, some information was gathered during previous audits performed by the OIG.

Based on the information provided, we determined NARA has policies and procedures in place for logical access controls, including the use of multifactor authentication for privileged users to access covered systems, and data security management practices for NARA and other entities including contractors. However, NARA has not implemented and followed its process and procedures for some covered systems. For example, 18 of 30 of NARA-identified covered systems do not have multifactor authentication implemented for privileged users. NARA indicates many of these 18 systems are either not connected to the network, or hosted by a third-party. These systems require privileged users to access the covered system with a username and password. NARA's own IT Security Requirements document states users with elevated security privileges shall access the system using a multi-factor authentication mechanism that complies with applicable Federal directives and NARA policy. The 18 covered systems are not in compliance with NARA policy.

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, restitution, and other actions. The OI may also issue management letters detailing specific problems or vulnerabilities, and offering insight on how to correct them.

Significant Investigations and Updates

NARA's Public Transit Subsidy Program (PTSP)
Previously we reported several NARA employees faced potential disciplinary action from the agency for violating the terms of the Public Transit Subsidy Program. During this period, NARA terminated the employees. Moreover, suspensions have been proposed for other NARA employees in the chain of command for some of the terminated employees.

Unauthorized Outside Employment in the Workplace
Previously we reported on an employee who engaged in retail sales in the workplace to contractors and fellow employees, did not obtain permission to engage in outside employment, and used NARA information technology resources to advertise their retail business. During this period the agency took disciplinary action.

False Information on Employment Application Documents
Previously we reported that an employee submitted false information on their employment application documents, including false information pertaining to termination from previous employment, and criminal arrest history. Both Federal and state prosecutors declined prosecution in favor of administrative action. During this period, NARA terminated the employee.

Probationary Employee Terminated for Time and Attendance Fraud
We reviewed an allegation an employee consistently falsified their time and attendance record over several weeks. It was found they would arrive late, but did not stay late or take leave to cover the lost time. The employee was in a probationary status, and NARA terminated their employment during this period.

Veteran Falsifies Records for Federal Benefits
We received an allegation that a veteran obtained personal military records from NARA and altered them to make false statements indicating they had been serving on active-duty overseas in 2008 and 2009 when two properties they owned were foreclosed-upon. The investigation substantiated the subject used, among other items, an Officer's Performance Report and a letter purporting to be from an employee in the National Personnel Records Center in support of the fraud scheme, both of which were forgeries. The fraud was an attempt to gain protection under the *Servicemembers' Civil Relief Act*, which protects members of the Armed Forces from foreclosures in certain circumstances. If successful, the fraud would have gained the subject

approximately $730,000. In June 2016, the subject pleaded guilty to one charge of making a false statement. The subject is scheduled to be sentenced in January 2017 and, according to a press release issued by the Office of the United States Attorney, faces "a likely range of 24 to 30 months in prison and potential fine of $10,000 to $95,000."

Leavenworth Federal Penitentiary Inmate Photographs Recovered for NARA

We found Leavenworth Federal Penitentiary inmate photographs ("mugshots") that should be part of NARA's holdings were available for sale on *eBay*. We determined a Missouri law enforcement official came into possession of the photographs decades earlier. With the official's death, the photographs became part of their estate and were purchased by a legitimate dealer in such memorabilia, who in turn offered them for sale on *eBay*. Through our extensive coordination both with the dealer and with people who had already purchased some of the photographs, we were able to recover 42 of the 57 photographs. The recovered photographs are now in the custody of Research Services, and our efforts to locate and reclaim the remaining photographs continue.

Unauthorized Secondary Employment and Telework Abuse

We reviewed an allegation that, over the course of several years, a high-level employee abused their working hours, office network connection, and telework privilege by using substantial quantities of work time and network bandwidth to surf the internet, and conduct research for a book that was subsequently published. The investigation confirmed that from approximately January 2010 forward, the subject had appropriated disproportionately large quantities of network bandwidth on their office computer, and had spent thousands of working hours surfing the internet and researching the topic of their book. Our investigation established that, on their regular telework days, the subject had conducted 11, approximately hour-long, podcast interviews not related to their NARA work. As a function of the subject's salary and benefits, the total aggregate loss to the agency from the subject's wasted time was estimated to be approximately $200,000. The subject resigned.

Unauthorized Secondary Employment and Telework Abuse

We received an allegation that a high-level supervisor abused their twice-weekly telework privilege to run a family business. The investigation substantiated the allegation that on some days the subject teleworked from their family business, and occasionally the subject would be the sole business representative at the business when their spouse left to run errands. The subject also would occasionally meet with contractors for the family business during telework days. The subject also failed to make mandatory disclosures on their annual Office of Government Ethics Form 450. The subject resigned.

Viewing Pornography in the Workplace with Agency IT Equipment

We received an allegation an employee spent part of their NARA working day viewing pornographic imagery at work. The investigation substantiated the allegation. Since at least January of 2015, the employee, who had a high-level security clearance for their work at NARA, frequently used their work-issued computer to view inappropriate websites, including sites related to escort services, and to view pornographic images. When interviewed, the subject further admitted to scheduling appointments with escorts on several occasions, and to having met with a scheduled escort at least once. In response to our investigation, the agency revoked the

employee's security clearance and proposed termination. However, the employee instead resigned.

Significant Referrals

Contract Security Officer's Firearm Stolen from Residence

We reviewed an allegation that a contract security guard brought their company issued service pistol home in violation of the terms of the employing company's contract with NARA. We referred this matter back to the Security Management Division (BX) for review and action. BX substantiated the allegation, and determined that the officer mistakenly left their pistol in the trunk of their vehicle, wherefrom it was stolen sometime between the time they arrived home, and the following morning. The officer no longer works at a NARA facility.

Personal Use of Government Travel Credit Card

The OI's monthly review of NARA travel card purchases indicated that in June 2016, an employee of the Federal Records Centers misused their Government travel card to pay for more than a dozen personal, travel-related expenses. These included fuel, vehicle service, and lodging for personal travel relating to an employment search. We referred the matter to the agency for closer review, and in response the employee admitted to the misconduct. The employee was subsequently issued a Letter of Warning.

Ongoing Oversight

Erroneous Disclosure of Personally-Identifiable Information

Every month, the staff of the National Personnel Records Center (NPRC) processes literally *tens of thousands* of document requests from private citizens and from Government agencies such as the U.S. Department of Veterans' Affairs. In a very small number of cases, generally less than 0.02%, document recipients report receiving erroneous personally identifiable information pertaining to someone other than the requester. In these cases, NPRC reports its supervisors promptly issue remedial actions and progressive discipline to address the errors and to prevent similar errors from occurring again. In this reporting period, the NPRC issued seven Letters of Counseling, three Letters of Warning, and a single one-day suspension for erroneous disclosures. One employee resigned after receiving a Letter of Counseling.

NARA 802 Initiative – Employee Misuse of IT Resources

In this reporting period, the OI increased the scope and intensity of its initiative to develop researchable indicators of employee misuse of information technology equipment and other resources in violation of NARA 802: *Use and Monitoring of NARA Office and Information Technology (IT) Equipment and Resources*.

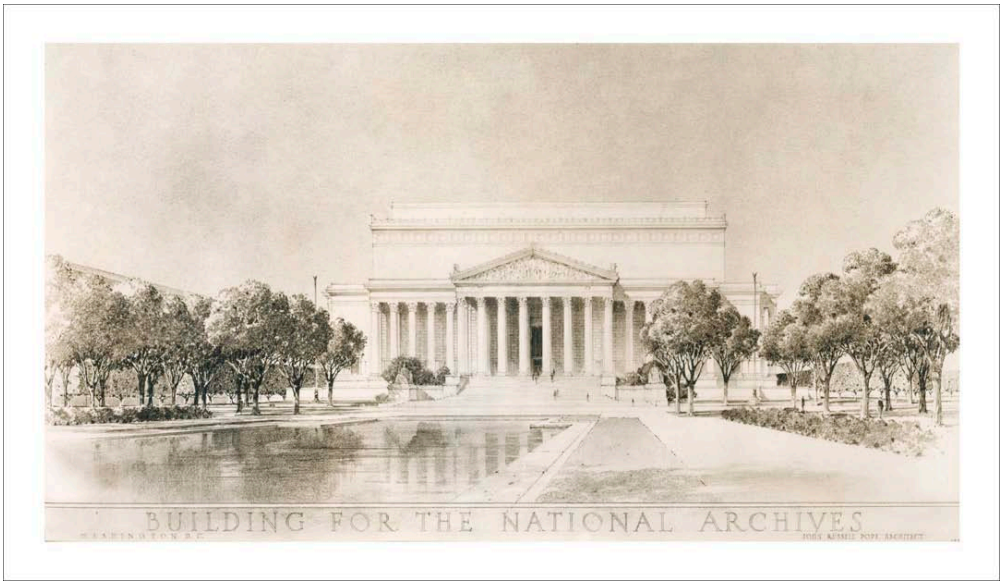
Our enhanced system reviews have identified numerous instances of employee misuse of IT equipment and resources, highlights of which include:

1. A contract employee was found to spend time during their working hours using a NARA-assigned computer to access escort-related websites and to view sexually-explicit images. In this case, the employing company removed the subject from the contract.

2. A contract employee engaged in daily recurring video streaming using their NARA-issued computer to watch entertainment programs. This activity required tremendous quantities of bandwidth for the non-work-related use. In this case, the employee received a Letter of Counseling, and the employing contract company was charged approximately $1,500 to cover the expense of the employee's unworked hours during the period of review.
3. Six employees in one workplace engaged in frequent workday video streaming from popular entertainment websites. In this case, each of the six employees received a Letter of Counseling.
4. A data transcriber drew significant bandwidth for video streaming. In this case, the employee received a Letter of Counseling.
5. An archives technician drew significant quantities of bandwidth for non-work-related use. In this case, the employee received a Letter of Reprimand.
6. For more than the past year, an employee spent part of their NARA working day viewing pornographic imagery at work. The agency proposed termination; however, the employee resigned in August 2016.

In all, in this reporting period our NARA 802 Initiative has resulted in:

Contract Employees Removed from Contract	1
Monetary Compensation from Contract Companies	$1,581.87
Letters of Counseling	8
Letters of Reprimand	1
Employee Resignations	1



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	252
Hotline and Complaints referred to NARA or another entity	60

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*.

SIGNIFICANT DISAGREEMENTS

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."

Federal Manager's Financial Integrity Act Reporting

Based upon our examination of NARA's FY 2016 Draft Federal Manager's Financial Integrity Act (FMFIA) statement and our assessment of NARA's internal controls for FY 2016, we do not concur with the agency assurance statement for Section 2 of the (FMFIA) reporting requirements. Specifically, NARA cannot provide reasonable assurance of effectiveness and efficiency over its operations. We acknowledge NARA continues to improve its internal control program. However, until NARA can effectively identify, test, and monitor all of the critical risks in program areas, NARA cannot provide reasonable assurance of effectiveness and efficiency over its operations.

The OIG conducted an FY16 Audit of NARA's Compliance with the Federal Managers' Financial Integrity Act for FY15 and found NARA did not develop and maintain effective internal control over its programs and activities; did not adhere to requirements of its own Internal Control Program (ICP); and did not prepare its final FY15 FMFIA Assurance Statement based on evaluation of internal controls. As a result, NARA remains unaware of potential risks and challenges to its programs and activities, and provided its final FY15 FMFIA Assurance Statement without adequate, sufficient, and reliable information to support its conclusion.

Additionally, the OIG engaged Cotton & Company LLP to perform an enterprise-wide risk assessment of NARA's internal controls and the risks to its operations and procedures. The audit found while NARA appears to be aware of the significant risks and challenges they face, NARA has yet to implement an enterprise-wide risk management (ERM) program that clearly identifies, prioritizes, and manages risks throughout the organization. NARA management has not made the implementation of an ERM program a strategic priority and instead has been relying on their ICP and Management Control Oversight Council to identify and manage risks throughout the organization. As a result, management's internal control activities and assurance statements continue to be based on work at the individual function, program, and office level. Findings and recommendations in both OIG audit reports coupled with the new requirements of the revised OMB Circular A-123 (July 2016), which established requirements for Enterprise Risk Management (ERM) in Executive agencies should assist NARA in developing an effective ERM program.

Refusal to Provide Information Access to the OIG

During this period NARA refused to allow the OIG independent access to employee emails to review them for potential violations of the Hatch Act. In management's opinion, the OIG should not be allowed "unfettered" access to NARA information, and management should be allowed to act as a gatekeeper to control the flow of information to the OIG.

In this instance, the OIG requested access to all NARA emails on the government system in

order to run computer searches for terms indicating potential violations of the Hatch Act. The Hatch Act limits certain political activities of Federal employees. Its purpose is to ensure Federal programs are administered in a nonpartisan fashion, protect Federal employees from political coercion in the workplace, and ensure Federal employees are advanced based on merit and not based on political affiliation. Among other things, almost all Federal employees may not use their official authority or influence to affect the result of an election; may not solicit donations for a partisan political party, group, or candidate; and may not engage in political activity while on duty or in any Federal room or building. Political activity is any activity directed at the success or failure of a political party, candidate for partisan political office, or political group.

When the OIG asked for access to the email system to search for potential violations, NARA refused. Management stated the OIG should only search for violations "based on information that a specific person or persons are engaged in misconduct." This stance by management does not line up with the OIG's statutory mission to prevent and detect fraud and abuse in NARA's programs and operations. However, at a subsequent meeting NARA then offered to run the searches itself if the OIG provided search terms, and NARA would provide the OIG with the results. While in the end NARA agreed to provide the information sought, we feel it is impermissible for the agency to actively interject itself into an OIG review and become the arbiter of if or how the OIG has access to NARA information.

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 was initially billed as storing 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 costs, 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 going forward. These include the growth in the amount and diversity of digital materials produced by government agencies; and 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 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.

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. Adding to the challenge is NARA's administrative structure as NARA's Chief Information Officer (CIO) does not report directly to the head of the agency. 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 2016 (with exceptions of 2013 and 2014, where it was downgraded to a reportable issue). In FY 2016, management identified control deficiencies in five IT Security-related areas (Authority to Operate, Desktop Baseline Configuration, Server Baseline Configuration, Patch Management, and Information Security Continuous Monitoring) that, when considered collectively, represent a material weakness.

In addition, annual assessments of NARA's compliance with the Federal Information Security Modernization Act (FISMA) 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 limits in 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. 44 U.S.C. § 2903 makes the Archivist responsible for the custody, control, operation, and protection of buildings used for the storage of Federal records. NARA-promulgated regulation 36 CFR Part 1234, "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

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

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 may still continue 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 which make 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, as NARA is challenged to maintain security, data reliability and accuracy, and manage personnel data and system access for individuals other than Federal employees.

10. Enterprise Risk Management

In July 2016, OMB updated its Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, to ensure Federal managers are effectively managing risks an agency faces toward achieving its strategic objectives and arising from its activities and operations. The Circular provides updated implementation guidance to Federal managers to improve accountability and effectiveness of Federal programs as well as mission support operations through implementation of Enterprise Risk Management (ERM) practices and by establishing, maintaining, and assessing internal control effectiveness. GAO has reported NARA has not established an ERM capability, thus reducing its ability to anticipate future challenges and avoid potential crises. Currently, the agency has not established a fully-effective internal control program. Thus, NARA is vulnerable to risks that may not be foreseen or mitigated, and does not have the ability to self-identify and appropriately manage or mitigate significant deficiencies. An effective ERM capability:

- creates and protects value;
- is an integral part of organizational processes and decision making;
- is dynamic, iterative, and responsive to change; and
- facilitates continual improvement of the organization.

NARA's challenge is to ensure the agency is in compliance with requirements of the updated OMB Circular A-123, and to develop and fully implement an ERM capability.

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	4–5 , 8
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, 34–64
Section 5(a)(3)	Prior significant recommendations unimplemented	33–64
Section 5(a)(4)	Summary of prosecutorial referrals	16–18, 30
Section 5(a)(5)	Information or assistance refused	21, 32
Section 5(a)(6)	List of audit, inspection, and evaluation 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	9
P.L. 110-181	Annex on completed contract audit reports	30
P.L. 104-106	Open audit recommendations	34–64

SUMMARY OF INVESTIGATIONS AND PROSECUTORIAL REFERRALS

Requirement 5(a)(4)

Investigative Workload	
Hotline and complaints received and opened this reporting period	252
Investigations opened this reporting period	13
Investigations closed this reporting period	17
Investigative Results	
Individuals referred – accepted for prosecution	0
Individuals referred – declined for prosecution	4
Individuals referred – pending prosecution decision	0
Arrest	1
Indictments and informations	1
Convictions	0
Fines, restitutions, judgments, and other civil and administrative recoveries	$1,581.87
Administrative Remedies	
Employee(s) terminated	5
Employee(s) resigned	4
Employee(s) suspended	2
Employee(s) given letter of reprimand or warnings/counseled	20
Employee(s) taking a reduction in grade in lieu of administrative action	0
Contractor (s) removed	1
Individual(s) barred from NARA facilities	0

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.

REPORTING REQUIREMENTS

LIST OF AUDIT, INSPECTION, AND EVALUATION REPORTS ISSUED

Requirement 5(a)(6)

Report No.	Title	Date	Questioned Costs	Unsupported Costs	Funds Put to Better Use
16-06	Audit of NARA's Preparation and Planning for the Receipt of President Obama's Administration's Records and Artifacts	4/19/2016	$0	$0	$0
16-07	Audit of NARA's Refile Processes at Selected FRCs	5/17/2016	$0	$0	$0
16-08	Audit of NARA's FY 2015 Compliance with Improper Payment Requirements	5/26/2016	$0	$0	$0
CR-16-1	Second Evaluation under the Reducing Over-Classification Act	5/12/2016	$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

REPORTING REQUIREMENTS

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

OTHER REQUIRED REPORTS

REQUIREMENT	CATEGORY	SUMMARY
5(a)(3)	Prior significant recommendations unimplemented	See pages 33–63.
5(a)(5)	Information or assistance refused	See page 21.
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 21–22.

Audit Recommendations Where NARA Has Assumed Risk

The following audit recommendations were closed by the OIG during this period as management has decided to assume the risk of not completely addressing the identified issues. While we believe our audit recommendations will help NARA's operations, the agency has decided appropriate controls are in place and the actions it has taken mitigate weaknesses and risks to an appropriate level. Previously the OIG did not close recommendations where management had decided to assume these risks, therefore the following list contains recommendations that NARA had assumed the risk for in prior periods.

Report No.	Audit Report Title	Rec #	Recommendation
08-01	Audit of NARA Artifacts	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.
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.
12-10	Follow up Audit of Artifacts	1h	Appropriate storage hardware for the Reagan Library is procured and installed.
12-10	Follow up Audit of Artifacts	6b	The Executive for Legislative Archives, Presidential Libraries, and Museum Services should establish reconciliation procedures between the completed inventories and White House legacy documentation for both Bush (42) and Obama Administrations as a compensating management control until the separation of duties issues at the Presidential Materials Division are mitigated.
12-10	Follow up Audit of Artifacts	6c	The Executive for Legislative Archives, Presidential Libraries, and Museum Services should ensure policy is developed for a security escort when picking up high-value object (HVO) gifts from the White House for courtesy storage at NARA.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.

Open Audit Recommendations[1]

An important responsibility of the OIG is to follow-up on previously issued audit reports with outstanding audit recommendations. The OIG, in concert with the agency, has implemented an improved audit process to work with management to close recommendations in a timely manner. During this reporting period 40 audit recommendations were either closed or subsumed into other recommendations.

Report No.	Audit Report Title	Rec #	Recommendation
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.
06-10	Evaluation of NARA's Affiliated Archives Program	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.
06-10	Evaluation of NARA's Affiliated Archives Program	5	The Archivist should ensure that all MOUs contain the required clause for the use of the NARA seal.
06-10	Evaluation of NARA's Affiliated Archives Program	6	The Archivist should ensure that all affiliates meet the current storage standards or provide waivers and/or 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.
08-02	Audit of NARA's Purchase Card Program	13	The Assistant Archivist of Administration should direct the Director of 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.
08-05	FY 07 FISMA Review	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.
08-05	FY 07 FISMA Review	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.

[1] As agreed upon by OIG and NARA, documentation provided by NARA within ten or more days of the end of the period was reviewed and considered for closure of open recommendations.

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	The CIO ensures that the WAHS meets OMB and NIST requirements prior to full implementation.
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.
10-04	Audit of NARA's Oversight of Electronic Records Management in the Federal Government	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.
10-04	Audit of NARA's Oversight of Electronic Records Management in 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.
10-04	Audit of NARA's Oversight of Electronic Records Management in the Federal Government	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.
10-04	Audit of NARA's Oversight of Electronic Records Management in the Federal Government	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.
10-04	Audit of NARA's Oversight of Electronic Records Management in the Federal Government	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.

10-07	Audit of NARA's Network Infrastructure	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.
10-14	Audit of the Process for Providing and Accounting for Information Provided to Researchers	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 apply the appropriate hot fix referenced in the vendor advisory on the affected machines.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	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.
11-02	Network and Penetration Testing Oversight	6a	NARA management immediately address corrective action for all vulnerabilities identified as "high" and "critical" risk.

11-02	Network and Penetration Testing Oversight	6b	NARA Management 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.
11-14	Audit of NARA's Foreign and Premium Travel	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.
11-14	Audit of NARA's Foreign and Premium Travel	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.
11-14	Audit of NARA's Foreign and Premium Travel	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.
11-15	Audit of NARA's Drug Testing Program	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.
11-15	Audit of NARA's Drug Testing Program	4	Develop a retention plan for all drug testing-related documentation consistent with the guidance issued by SAMHSA.
11-15	Audit of NARA's Drug Testing Program	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.
11-20	Audit of NARA's Telework Program	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.
11-20	Audit of NARA's Telework Program	3e	Review Citrix security configurations for adequacy.

12-05	Audit of the Management of Records at the Washington National Records Center	5	The Executive of 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.
12-05	Audit of the Management of Records at the Washington National Records Center	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.
12-05	Audit of the Management of Records at the Washington National Records Center	8	The Executive of Agency Services should ensure management designs and implements monitoring activities for records processed at WNRC including weekly, monthly, and quarterly reports.
12-05	Audit of the Management of Records at the Washington National Records Center	9c	A monitoring process is implemented for ensuring classified operations are performed as written in the Classified SOP.
12-05	Audit of the Management of Records at the Washington National Records Center	12a	Procedures for all WNRC processes are documented. Review existing procedures and update as necessary.
12-05	Audit of the Management of Records at the Washington National Records Center	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.
12-09	Audit of NARA's Data Center Consolidation Initiative	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.
12-09	Audit of NARA's Data Center Consolidation Initiative	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.

12-09	Audit of NARA's Data Center Consolidation Initiative	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.
12-09	Audit of NARA's Data Center Consolidation Initiative	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.
12-09	Audit of NARA's Data Center Consolidation Initiative	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	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.
12-10	Follow up Audit of Artifacts	1c	The Reagan Library has taken all appropriate actions to resolve the 1,700 identified anomalies in order to complete Recommendation 5b from prior audit report OIG #08-01.
12-10	Follow up Audit of Artifacts	2b	Review and revise current time-guidance policy, as appropriate, for baseline inventories for newly established Presidential libraries.
12-10	Follow up Audit of Artifacts	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.
12-10	Follow up Audit of Artifacts	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.
12-10	Follow up Audit of Artifacts	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.
12-10	Follow up Audit of Artifacts	7c	Reiterate NARA policy to adequately backup inventory-related collection documentation.
12-10	Follow up Audit of Artifacts	8a	Update comprehensive set of museum collection management policies and procedures and ensure their development.
12-10	Follow up Audit of Artifacts	8b	Establish procedures to periodically review and, if necessary, revise said policies and procedures.
12-11	NARA's Network Assessment Audit	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.

12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.

12-11	NARA's Network Assessment Audit	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.
12-11	NARA's Network Assessment Audit	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.
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.
12-15	Audit of NARA's Classified Systems	2	I, in coordination with C, should establish a timeframe for review and approval of authorization documents.
12-15	Audit of NARA's Classified Systems	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.
12-15	Audit of NARA's Classified Systems	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.
12-15	Audit of NARA's Classified Systems	7a	I, in coordination with C, should provide appointment letters for the SOs and ISSOs.
12-15	Audit of NARA's Classified Systems	7c	I, in coordination with C, should provide a sample of reading and record copies of signed appointment letters.
12-15	Audit of NARA's Classified Systems	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.
13-01	Audit of NARA's Internal Controls Program for FY 2010	1e	Risk management responsibilities are included in the performance plans for program and function owners.
13-01	Audit of NARA's Internal Controls Program for FY 2010	1f	Prior recommendations from previous OIG and GAO reports are closed.
13-01	Audit of NARA's Internal Controls Program for FY 2010	1g	A Risk Management Policy is created to communicate NARA's commitment to enterprise risk management.
13-01	Audit of NARA's Internal Controls Program for FY 2010	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.

13-08	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.
13-08	Audit of NARA's Preservation Program (Textual)	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.
13-08	Audit of NARA's Preservation Program (Textual)	2	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services, should ensure comprehensive preservation policies and procedures for each of their organizations are developed and/or updated.
13-08	Audit of NARA's Preservation Program (Textual)	3a	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services should completely identify the resources necessary to adequately accomplish NARA's preservation mission.
13-08	Audit of NARA's Preservation Program (Textual)	3b	Develop a plan to identify the complete universe of textual and non-textual records that require preservation.
13-08	Audit of NARA's Preservation Program (Textual)	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.
13-08	Audit of NARA's Preservation Program (Textual)	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.
13-08	Audit of NARA's Preservation Program (Textual)	5b	The Executive for Research Service should ensure additional measurable performance metrics are developed and implemented to track the progress within the Preservation Program.
13-08	Audit of NARA's Preservation Program (Textual)	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.
13-08	Audit of NARA's Preservation Program (Textual)	5d	The Executive for Research Services should ensure Denver, St. Louis, and Special Media implement HMS to record risk assessments.

13-08	Audit of NARA's Preservation Program (Textual)	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	4	The CIO should develop a process to regularly test data backups to verify information integrity.
13-09	NARA's Data Backup Operations	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.
13-10	NARA Archival Facilities	1b	The COO should ensure a plan is developed including a timeline for when the archival storage facility reviews will be completed.
13-10	NARA Archival Facilities	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.
13-10	NARA Archival Facilities	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.
13-10	NARA Archival Facilities	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 assesses Federal agency usage of Base ERA and implements 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 into Base ERA.
13-11	Audit of ERA Ingest Efforts	2	The COO identifies the most efficient and effective method of ingest and requires 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.

13-12	Audit of the NARA IDS	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.
13-12	Audit of the NARA IDS	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 Processing of Textual Records	2b	The Executive of 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.
13-14	Audit of Processing of Textual Records	2c	The Executive of 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.
13-14	Audit of Processing of Textual Records	2d	The Executive of Research Services should conduct a workload analysis to determine if resource allocation between AI and AII is appropriate.
13-14	Audit of Processing of Textual Records	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.
13-14	Audit of Processing of Textual Records	3b	The Executive for Legislative Archives, Presidential Libraries and Museums should (a) analyze the backlogs at the pre-PRA libraries and create processing plans for reducing the backlogs at these libraries on a more accelerated basis; (b) assess if there are additional ways to accelerate processing at the PRA libraries; (c) work with the Performance and Accountability Office to update the PMRS metadata to require an ARC entry prior to considering Presidential records processed.
13-14	Audit of Processing of Textual Records	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.
13-14	Audit of Processing of Textual Records	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.
13-14	Audit of Processing of Textual 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.

13-14	Audit of Processing of Textual Records	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.
13-14	Audit of Processing of Textual Records	7	The Executive of Research Services should ensure procedures for all field locations are documented. Review existing procedures and update as necessary.
13-14	Audit of Processing of Textual Records	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.
14-04	Audit of the Use of Presidential Libraries by Outside Organizations	5	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.
14-05	Audit of NARA's Field Offices Acquisition Activity	1b	NARA should consider terminating field office contracting officers' warrants until all initial training requirements are met.
14-05	Audit of NARA's Field Offices Acquisition Activity	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.
14-05	Audit of NARA's Field Offices Acquisition Activity	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.
14-05	Audit of NARA's Field Offices Acquisition Activity	4	Update NARA policies to ensure the guidance for approval of small and small disadvantaged business utilization exceptions is consistent.

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.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process	1b	The CIO should ensure all required CPIC related documentation is completed for all NARA IT investments going through the CPIC process.
14-08	Audit of NARA's Capital Planning and Investment Control (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.
14-08	Audit of NARA's Capital Planning and Investment Control (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.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process	3	The Chief Operating Officer (COO) should ensure NARA IT investments do not bypass NARA's CPIC process.
14-08	Audit of NARA's Capital Planning and Investment Control (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.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process	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.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process	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.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process	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.
14-09	Audit of Conference-Related Activities and Expenses	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.

14-09	Audit of Conference-Related Activities and Expenses	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.
14-10	Audit of NARA's Enterprise Wireless Access	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.
14-10	Audit of NARA's Enterprise Wireless Access	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.
14-10	Audit of NARA's Enterprise Wireless Access	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.
14-10	Audit of NARA's Enterprise Wireless Access	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.
14-10	Audit of NARA's Enterprise Wireless Access	4a	NARA should utilize existing WLC and WAP baseline configurations or develop its own baseline configurations.
14-10	Audit of NARA's Enterprise Wireless Access	4b	NARA should implement a process to monitor the WLC and WAP settings for compliance with the established baseline configurations.
14-10	Audit of NARA's Enterprise Wireless Access	4c	NARA should document and approve any deviations from the WLC and WAP baseline configurations.
14-10	Audit of NARA's Enterprise Wireless Access	4d	NARA should maintain older versions of the baseline configurations as necessary.
14-10	Audit of NARA's Enterprise Wireless Access	5a	NARA should implement a process to conduct vulnerability scans that identify weaknesses related to NARA's wireless environment.
14-10	Audit of NARA's Enterprise Wireless Access	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.
14-11	Audit of Special Telework Arrangements at NARA	2	The CHCO should provide clarifying guidance to supervisors as to which arrangements require executive or staff director approval.
14-11	Audit of Special Telework Arrangements at NARA	3	The CHCO should establish an oversight mechanism to ensure employees' duty station assignments are reviewed and validated periodically.
14-11	Audit of Special Telework Arrangements at NARA	4	The CHCO should seek reimbursement of the $4,447 overpayment, or grant a waiver in accordance with 5 U.S.C. 5584.
14-11	Audit of Special Telework Arrangements at NARA	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.
14-11	Audit of Special Telework Arrangements at 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 timeframe for the arrangement, while still subject to the annual renewal.
14-11	Audit of Special Telework Arrangements at NARA	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.
14-11	Audit of Special Telework Arrangements at NARA	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.
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.

15-01	Audit of FISMA for FY 2013	2	Coordinate with the Office of Performance and Accountability and the 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.
15-02	Audit of NARA Mobile Security	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.
15-02	Audit of NARA Mobile Security	1c	Develop and document a strong internal control process for determining when an additional charge will be considered for reimbursement.
15-02	Audit of NARA Mobile Security	2	Review and update NARA's current policy documents for use of NARA-issued mobile devices, including NARA 813-1 and NARA 802 to reflect more complete and accurate information on acceptable uses of the devices and when a disciplinary action will be requested.
15-02	Audit of NARA Mobile Security	3	Provide training to educate users on acceptable uses of NARA-issued mobile devices, including requesting a travel device for international travel.
15-02	Audit of NARA Mobile Security	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.
15-02	Audit of NARA Mobile Security	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.
15-02	Audit of NARA Mobile Security	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.
15-02	Audit of NARA Mobile Security	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.
15-02	Audit of NARA Mobile Security	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 Holdings	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.
15-03	Audit of Specially Protected Holdings	2a	Security Management performs initial certifications of Specially Protected Holdings (SPHs) storage areas.

15-03	Audit of Specially Protected Holdings	2b	Security Management performs security inspections of SPHs storage areas.
15-03	Audit of Specially Protected Holdings	2c	Security Management develops guidelines for SPHs security inspections, including timeframes, criteria, documenting requirements, and reporting requirements.
15-03	Audit of Specially Protected Holdings	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.
15-03	Audit of Specially Protected Holdings	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.
15-03	Audit of Specially Protected Holdings	5a	Ensure 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.
15-03	Audit of Specially Protected Holdings	5b	Ensure inventory listings are reviewed to determine their accuracy and update as necessary.
15-03	Audit of Specially Protected Holdings	5c	Ensure a finding aid is created for the agency's entire SPHs collection at the item level.
15-03	Audit of Specially Protected Holdings	5d	Ensure locked hard copies of the inventory listings are maintained.
15-03	Audit of Specially Protected Holdings	5e	Ensure SPHs inventory listings are maintained in the Holdings Management System (HMS). Until HMS is implemented by all offices, ensure all electronic versions of the listings are password protected and access limited to authorized employees.
15-03	Audit of Specially Protected Holdings	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.
15-03	Audit of Specially Protected Holdings	7	Ensure all Presidential Libraries are in compliance with NARA 1572 policy of conducting annual inspections.
15-03	Audit of Specially Protected Holdings	8a	Initial inspections of SPHs inventory are completed.
15-03	Audit of Specially Protected Holdings	8b	Custodial units are in compliance with NARA 1572, including randomly inspecting at least 3% of SPHs inventory annually on a rotating basis and using one individual that does not work for the individual responsible for the inspection.
15-03	Audit of Specially Protected Holdings	8c	Annual inspection reports include at a minimum date of inspection, individuals that complete the inspections, and a listing of items inspected, including their location and physical condition.

15-03	Audit of Specially Protected Holdings	8d	Annual inspection results are adequately documented and communicated to Security Management and office heads.
15-03	Audit of Specially Protected Holdings	9a	Staff is properly trained or retrained to use charge out cards whenever records are removed from SPHs storage areas.
15-03	Audit of Specially Protected Holdings	9b	Access to SPHs storage areas is properly monitored, including keeping the list for who has access to the SPHs areas updated at all times and restricting access to only authorized staff.
15-03	Audit of Specially Protected Holdings	10a	Required elements for the handling of SPHs for each record storage area should be communicated to each custodial unit.
15-03	Audit of Specially Protected Holdings	10b	Detailed procedures are documented for each custodial unit.
15-03	Audit of Specially Protected Holdings	10c	A process is in place for periodic review of procedures and updates are made as needed.
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.
15-10	Audit of Digitization Partnership Process	2	Establish criteria for which Digitization Partnerships require public notification and approval by the Archivist of the United States.
15-10	Audit of Digitization Partnership Process	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	4	Develop agency-wide policies and procedures for digital file preservation.
15-11	Audit of Digitization Storage	6	Develop a long-term strategy for increasing transfer capabilities between various internal storage systems housing digitized records.
15-11	Audit of Digitization Storage	7	Develop a long-term storage strategy for currently held partner data and partner data to be provided to NARA in the future.
15-11	Audit of Digitization Storage	8	Work with partners to return partner-provided hard drives.
15-11	Audit of Digitization Storage	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.
15-11	Audit of Digitization Storage	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.
15-13	Audit of HR Systems and Data Accuracy	4a	Create an Employee Locator update policy including a defined timeframe within which employees are required to review and update Employee Locator entries.
15-13	Audit of HR Systems and Data Accuracy	4b	Create an Employee Locator update policy including supervisors' responsibility to ensure employee contact information remains complete and accurate

15-13	Audit of HR Systems and Data Accuracy	5	Include in the new hire orientation the requirement to update Employee Locator entries, based on the policy created from recommendation three.
15-13	Audit of HR Systems and Data Accuracy	9a	Ensure user accounts for separated employees are removed in a timely manner.
15-13	Audit of HR Systems and Data Accuracy	9b	Ensure roles and privileges assigned to the users are commensurate with their current job responsibilities.
15-13	Audit of HR Systems and Data Accuracy	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.
15-13	Audit of HR Systems and Data Accuracy	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.
15-14	Audit of Space Management for Paper Records	2	Implement a strategy to work with other Federal agencies to resolve "limbo" records and schedule those records for accessioning or disposal.
15-14	Audit of Space Management for Paper Records	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.
15-14	Audit of Space Management for Paper Records	4	Establish a permanent group to both track and manage space and advise NARA management on space matters across the agency.
15-14	Audit of Space Management for Paper Records	5	Develop a long-term space management strategy for the agency.
15-14	Audit of Space Management for Paper Records	6	Develop cost estimates for potential solutions.
15-14	Audit of Space Management for Paper Records	7	Incorporate space management into NARA's strategic planning initiatives and include the agency's space need in all necessary reporting. Consider reporting space management as a Material Weaknesses and track it appropriately
15-14	Audit of Space Management for Paper Records	8	Create a timeline for the agency to have necessary discussions with both internal and external stakeholders to address NARA's space challenges.
15-14	Audit of Space Management for Paper Records	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 should incorporate all locations into the NARANet SA&A package by documenting location-specific security controls and ensuring that they are appropriately tested and monitored.

15-15	Cabling Audit	2.1	Ensure that neat cable management and labeling mechanisms are employed for all sites.
15-15	Cabling Audit	2.2	Ensure that all server rooms are equipped with appropriate fire detection and suppression capabilities.
15-15	Cabling Audit	2.3	Limit access to all server rooms to those individuals with an explicit need to access IT equipment.
15-15	Cabling Audit	2.4	Ensure that appropriate temperature and humidity monitoring and control mechanisms are employed for all server rooms.
15-15	Cabling Audit	2.5	Ensure that appropriate UPS devices are employed for hardware supporting the site's network infrastructure.
15-15	Cabling Audit	2.6	Ensure that all server racks, switches, and network equipment are adequately secured from unauthorized access via locked racks.
15-15	Cabling Audit	3	NARA should 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.
16-01	Audit of NARA's Web Hosting Environment	1	The Chief Operating Officer (COO) should coordinate with the Chief Innovation Officer (CINO) to clearly define a business owner for the public facing website process
16-01	Audit of NARA's Web Hosting Environment	2	The COO should coordinate with the CIO, Office of Presidential Libraries and the CINO to develop and document a centralized process to manage the public facing websites
16-01	Audit of NARA's Web Hosting Environment	3	The CIO and CINO clearly define the roles and responsibilities throughout the process developed in recommendation #2
16-01	Audit of NARA's Web Hosting Environment	4	The COO should coordinate with the CINO to develop a comprehensive list of public facing websites.
16-01	Audit of NARA's Web Hosting Environment	5	The CIO and NGC should review and document the approval of all agreements for web hosting services.
16-01	Audit of NARA's Web Hosting Environment	6	The CIO should review all of the systems attached to the NARANet general support system to determine if there are any others that are not FISMA compliant.
16-01	Audit of NARA's Web Hosting Environment	7	The CIO should coordinate with the CINO to make the web hosting environment FISMA compliant.
16-01	Audit of NARA's Web Hosting Environment	8	The COO should coordinate with the CIO and CINO to evaluate whether all of the web hosting environments (internal and external) should be consolidated into one centralized system for FISMA purposes.
16-01	Audit of NARA's Web Hosting Environment	9	The CIO should develop and document a process by which Information Services regularly communicates (no less than monthly) with Innovation.

16-01	Audit of NARA's Web Hosting Environment	10	The CIO should provide Innovation with guidance that clearly delineates the management responsibilities of the web hosting environment between Information Services and Innovation.
16-01	Audit of NARA's Web Hosting Environment	11	The CIO should provide training to Innovation regarding their responsibility as a System Owner.
16-01	Audit of NARA's Web Hosting Environment	12	The CIO, COO, and CINO should retroactively perform or obtain from the contractor, vendor, or partner IT security assessments on vendors that currently host NARA websites.
16-01	Audit of NARA's Web Hosting Environment	13	The CIO should require an IT security assessment be performed prior to NARA initiating a web hosting agreement.
16-01	Audit of NARA's Web Hosting Environment	14	The CIO should ensure that all IT service agreements with external contractors, vendors, or partners have a clause that requires NARA or an independent third-party contractor to annually perform IT security assessments on contractor's, vendor's and partner's external web hosting environment(s) that host NARA websites.
16-01	Audit of NARA's Web Hosting Environment	15	The CIO should ensure Information Services personnel document their review of the IT security assessments.
16-01	Audit of NARA's Web Hosting Environment	16	The CIO should ensure Information Services include an audit clause in the agreement that requires contractors, vendors, and partners to provide all documentation to the OIG without requiring a signed NDA.
16-01	Audit of NARA's Web Hosting Environment	17	Develop a process for managing access to shared user accounts.
16-01	Audit of NARA's Web Hosting Environment	18	Implement the annual compliance check required by the User Account Management Standard Operating Procedure for Administrator accounts to the shared user accounts.
16-01	Audit of NARA's Web Hosting Environment	19	Coordinate with Information Services to develop and document a plan to recover the other NARA hosted websites besides Archives.gov.
16-01	Audit of NARA's Web Hosting Environment	20	Develop a plan to test the contingency plan. Further we recommend the plan should be tested annually, as required by NARA's IT Security Methodology for Contingency Planning.
16-01	Audit of NARA's Web Hosting Environment	21	The CIO in coordination with the CINO should update the Disaster Recovery plan to include all of the steps necessary to recover the Archives.gov website.
16-01	Audit of NARA's Web Hosting Environment	22	The CIO should encrypt NARANet backup tapes.
16-01	Audit of NARA's Web Hosting Environment	23	Develop a current baseline configuration for the Solaris web servers.
16-01	Audit of NARA's Web Hosting	24	Apply the baseline configuration to the web servers.

	Environment		
16-01	Audit of NARA's Web Hosting Environment	25	Coordinate with Innovation to configure the WebStage server to mirror the production web servers.
16-01	Audit of NARA's Web Hosting Environment	26	The CIO should require all systems develop a baseline configuration document and have it approved before it is applied to the entire system.
16-01	Audit of NARA's Web Hosting Environment	27	The CIO should develop controls to ensure all deliverables are provided before a RFC/RFW ticket for the web hosting environment is closed.
16-01	Audit of NARA's Web Hosting Environment	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.
16-01	Audit of NARA's Web Hosting Environment	29	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
16-01	Audit of NARA's Web Hosting Environment	30	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
16-01	Audit of NARA's Web Hosting Environment	31	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
16-01	Audit of NARA's Web Hosting Environment	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.
16-01	Audit of NARA's Web Hosting Environment	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.
16-02	Audit of NARA's Compliance with FISMA, As Amended	1	NARA should develop and implement formalized procedures to ensure for those systems utilized by NARA and managed by Cloud Service Providers, controls for which NARA has a shared responsibility should be reviewed on an annual basis, documented and assessed as to the impact to NARA of any risks that may be present.
16-02	Audit of NARA's Compliance with FISMA, As Amended	2	NARA should complete the development, approval and deployment of baseline configurations which are currently in progress and ensure that systems are configured in accordance with best practices (including NIST-approved baselines), to include, but not limited to, always changing default credentials at the time of implementation.
16-02	Audit of NARA's Compliance with FISMA, As Amended	3	NARA should configure RRS application password settings in accordance with NARA policy
16-02	Audit of NARA's Compliance with FISMA, As Amended	4	NARA should develop, update, and implement formalized access control policies and procedures for the B&A, RRS, SCTS and DCU systems.

16-02	Audit of NARA's Compliance with FISMA, As Amended	5	NARA should implement and document user access reviews for B&A, ENOS/HMS, RRS, SCTS, and DCU.
16-02	Audit of NARA's Compliance with FISMA, As Amended	6	NARA should develop and implement procedures to reissue shared/group account credentials when individuals are removed from B&A and RRS user groups.
16-02	Audit of NARA's Compliance with FISMA, As Amended	7	NARA should establish and implement a formalized process for identifying NARANet accounts that are inactive after 90 days and disable if no longer needed.
16-02	Audit of NARA's Compliance with FISMA, As Amended	8	NARA should develop, update, and implement formalized VPN access policies and procedures to ensure individuals are granted appropriated access.
16-02	Audit of NARA's Compliance with FISMA, As Amended	9	NARA should establish and implement a formal process to create, assign, track, and remediate identified weaknesses in accordance with NARA-established requirements to: · Ensure milestone dates are updated as needed if targeted dates are expected to be missed or are overdue, while still documenting original targeted completion dates. · Investigate and complete actions and milestones to close out overdue POA&M items, specifically items with a medium risk level or higher
16-02	Audit of NARA's Compliance with FISMA, As Amended	10	NARA should implement OMB A-130 and NARA IT Security Requirement which require regular reviews and updates of system security plans and policies and procedures to address NIST 800-53, Revision 4 requirements and address related POA&M milestones.
16-02	Audit of NARA's Compliance with FISMA, As Amended	11	NARA should implement improved processes to continuously identify and remediate security deficiencies on NARA's network infrastructure to include enhancing its patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's applications and network infrastructure.
16-02	Audit of NARA's Compliance with FISMA, As Amended	12	NARA should develop, update and implement configuration management policies and system-specific configuration management plans which were either not developed or out-of-date.
16-02	Audit of NARA's Compliance with FISMA, As Amended	13	For future agreements, NARA should: · require that providers of external information system services comply with NARA information security requirements. · define and document government oversight and user roles and responsibilities with regard to external information systems, and. · establish a process to monitor security control compliance by external service providers on an ongoing basis.
16-02	Audit of NARA's Compliance with FISMA, As Amended	14	NARA should add an addendum to current agreements which requires compliance with NARA's information security requirements.

16-02	Audit of NARA's Compliance with FISMA, As Amended	15	NARA should develop and implement procedures to ensure all individuals with security roles and responsibilities are provided with adequate security-related technical training specifically tailored for their assigned duties on an annual basis.
16-02	Audit of NARA's Compliance with FISMA, As Amended	16	NARA should develop contingency plans and disaster recovery plans for SCTS and B&A, and any other systems identified as critical.
16-02	Audit of NARA's Compliance with FISMA, As Amended	17	NARA should review and update the RRS, NARA COOP/Disaster Recovery Infrastructure Specification and Rocket Center Network Design document, and DCU contingency plans and disaster recovery plans as necessary, and institute procedures to ensure annual reviews and updates of these documents for these systems and any other systems identified as critical.
16-02	Audit of NARA's Compliance with FISMA, As Amended	18	NARA should test the B&A, ENOS/HMS, RRS, DCU and SCTS system contingency plans for these and any other systems identified as critical once these documents have been developed and updated; and test tape backup information to verify media reliability and information integrity on a regular basis.
16-02	Audit of NARA's Compliance with FISMA, As Amended	19	NARA should establish and document a detailed process to perform a comprehensive annual information system component inventory count.
16-02	Audit of NARA's Compliance with FISMA, As Amended	20	NARA should implement the following corrective actions: · Complete efforts to implement the Net IQ Sentinel product; · Develop and implement processes and procedures to monitor and at least weekly review user activity and audit logs (in accordance with NARA IT Security Requirements), on the network, RRS, B&A, ENOS-HMS and DCU systems that may indicate potential security violations; and · Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging controls and functionality in accordance with NARA's IT Security Requirements, AU-2.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1a	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to determining the appropriate location of the system servers.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1b	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, determining if the servers and systems have the appropriate security protocols in place, including NARA standard software.

16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1c	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and federal guidelines, including, but not limited to, reviewing user lists and determining the appropriate access for each account and eliminating any accounts no longer needed.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1d	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, implementing NARA password requirements.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1e	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, limiting users' ability to perform data extracts and ability to use portable devices.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1f	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, determining how to properly backup the systems and store the backup tapes.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1g	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, determining how to properly monitor user activity, including audit logs.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	1h	Evaluate the electronic tracking and inventory systems and implement proper security controls according to NARA policies and Federal guidelines, including, but not limited to, ensuring all users have individual user accounts and passwords and do not share this information.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	2	Establish a process for the Field Office System Administrator to service standalone databases maintained at FRCs, including the IRS and DHS electronic inventory systems.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	3	Document procedures for the security of the IRS and DHS electronic tracking and inventory systems, including, but not limited to, access, backup and recovery, data extracts, and audit logs.

16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	4	Ensure control procedures under NARA Directive 1608, Protection of Personally Identifiable Information (PII), are followed.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	5a	Coordinate with NARA's Security Management Division to implement enhanced physical security controls for the AFOW-LX cold storage facility, including, but not limited to Performing a security risk assessment to determine if the facility is properly secured.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	5b	Coordinate with NARA's Security Management Division to implement enhanced physical security controls for the AFOW-LX cold storage facility, including, but not limited to Installing additional security measures to properly secure the records (e.g. door, locks, card reader, and cameras).
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	5c	Coordinate with NARA's Security Management Division to implement enhanced physical security controls for the AFOW-LX cold storage facility, including, but not limited to, implementing a log to properly monitor individuals entering and exiting the facility.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	6	Ensure all Federal Records Centers are following key control procedures under NARA Directive 271, Key Control at NARA Facilities
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7a	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, determining the appropriate location of the system server.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7b	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, determining if the server and system has the appropriate security protocols in place, including NARA standard software.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7c	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, reviewing user lists and determining the appropriate access for each account and eliminate any accounts no longer needed.

16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7d	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, implementing NARA password requirements.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7e	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, determining how to properly backup the system and store the backup tapes.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7f	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, determining how to properly monitor user activity, including audit logs.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	7g	Coordinate with NARA's Chief Information Officer and enhance information security controls for the AFOW-LX cold storage facility access system according to NARA policies and Federal guidelines, including, but not limited to, ensuring all users have individual user ids and passwords and do not share this information.
16-03	Inadequate Information and Physical Security Controls at Select Federal Records Centers	8	Provide only authorized users access to the cold storage system.
16-05	Audit of NARA's Publicly-Accessible Websites	1a	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinate with the CIO on the development of policies and procedures for secure website design and implementation that apply to all NARA publicly-accessible websites.
16-05	Audit of NARA's Publicly-Accessible Websites	1b	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinate with the CIO to ensure all publicly-accessible websites are compliant with NIST SP 800-53 revision 4.
16-05	Audit of NARA's Publicly-Accessible Websites	1c	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO regularly (at least quarterly) conducts a comprehensive web vulnerability scan on all NARA publicly-accessible websites.

16-05	Audit of NARA's Publicly-Accessible Websites	1d	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO documents the process conducting a web vulnerability scan on all publicly-accessible websites.
16-05	Audit of NARA's Publicly-Accessible Websites	1e	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO provides the necessary training to IT Security personnel to be able to review and interpret the vulnerability scanner results.
16-05	Audit of NARA's Publicly-Accessible Websites	1f	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO prevents users from saving their credentials in web browsers.
16-05	Audit of NARA's Publicly-Accessible Websites	1g	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO requires all NARA publicly-accessible websites to apply NARA's password configuration requirements.
16-05	Audit of NARA's Publicly-Accessible Websites	1h	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO requires all publicly-accessible websites to only send cryptographically protected user credentials.
16-05	Audit of NARA's Publicly-Accessible Websites	1i	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO requires users to change their passwords after a website password reset.
16-05	Audit of NARA's Publicly-Accessible Websites	1j	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO analyzes all publicly-accessible websites to determine if they are vulnerable to all variations of cross-site scripting including reflected.
16-05	Audit of NARA's Publicly-Accessible Websites	1k	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinates with the CIO to review all publicly-accessible websites for any potential information that could affect NARA's IT security posture.

16-05	Audit of NARA's Publicly-Accessible Websites	1l	The CINO coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the NARA General Counsel coordinates with the CIO and CINO on the publishing of the NARA employee directory and Government credit cardholders list to ensure the security of NARA employees is taken into consideration.
16-05	Audit of NARA's Publicly-Accessible Websites	2	The CIO develop guidance for securely configuring HTTPS.
16-05	Audit of NARA's Publicly-Accessible Websites	3	The CIO implement secure HTTPS configurations for all publicly-accessible websites.
16-05	Audit of NARA's Publicly-Accessible Websites	4	The CIO regularly scan (at least quarterly) all publicly-accessible websites to determine if HTTPS is securely configured.
16-05	Audit of NARA's Publicly-Accessible Websites	5	The CIO document a process to review all security assessments by a qualified official.
16-05	Audit of NARA's Publicly-Accessible Websites	6	The CIO ensure Information Services personnel review all cloud hosting security assessments.
16-05	Audit of NARA's Publicly-Accessible Websites	7	The CIO ensure Information Services personnel document their review of the IT security assessments.
16-06	Re-issued - NARA's Preparation and Planning for the Receipt of President Obama's Administration's Records and Artifacts	2	The Chief Information Officer develop a contingency plan that could be activated to ensure responses to special access requests occur in a timely manner, in the event the ERA EOP System is not able to comply with the PRA.
16-07	NARA's Refile Processes at Selected Federal Records Centers	1	The Executive for Agency Services develop a plan to eliminate the backlog at each FRC.
16-07	NARA's Refile Processes at Selected Federal Records Centers	2	The Executive for Agency Services initiate onsite reviews at a named FRC and any other FRCs with unverified physical inventories to determine the extent of the IRS backlog, including performing physical inventories of IRS records awaiting refile, documenting dates received, and updating weekly inventory reports.
16-07	NARA's Refile Processes at Selected Federal Records Centers	3	The Executive for Agency Services develop a plan to eliminate the backlog at each FRC; create standardized FRC policies and procedures to process IRS records to meet timeframe requirements and accurately report IRS refile times and volumes to include enhancing controls to review all reports prior to sending to the IRS.

16-07	NARA's Refile Processes at Selected Federal Records Centers	4	The Executive for Agency Services coordinate with the IRS to receive more detailed information, including record listings, to allow for improved tracking of IRS records at FRCs.
16-07	NARA's Refile Processes at Selected Federal Records Centers	5	The Executive for Agency Services establish standardized procedures for verifying batch volumes.
16-07	NARA's Refile Processes at Selected Federal Records Centers	6	The Executive for Agency Services coordinate with the Director of the specific FRC to make all necessary reports concerning the missing record.
16-07	NARA's Refile Processes at Selected Federal Records Centers	7	The Executive for Agency Services update the batch signoff process requiring employees to attest every item included in a batch was properly refiled or interfiled.
16-07	NARA's Refile Processes at Selected Federal Records Centers	8	The Executive for Agency Services implement consistent unique batch numbering processes at the FRCs.
16-07	NARA's Refile Processes at Selected Federal Records Centers	9	The Executive for Agency Services implement standard IRS document locators at the FRCs.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10a	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including the selection criteria and quality control sample percentage to ensure the quality and timeliness of the quality control review.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10b	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including physically checking some percentage of refiles selected for review to ensure they were properly refiled.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10c	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including establishing timeframes for when the reviews must be conducted.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10d	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including documenting reviews performed, including records selected, errors identified, preparer and reviewer sign-off, and notification to employees and supervisors.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10e	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including Determining the appropriate method for reviewing interfiles.

16-07	NARA's Refile Processes at Selected Federal Records Centers	10f	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including ensuring different employees are responsible for the batching, selecting the quality control sample, refiling, and quality control review of records.
16-07	NARA's Refile Processes at Selected Federal Records Centers	10g	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including a mechanism for tracking errors identified by employee and conducting periodic training when consistent errors are identified.
16-07	NARA's Refile Processes at Selected Federal Records Centers	11	The Executive for Agency Services conduct training for all employees on the policies and procedures for quality control reviews, including notification of errors and penalties.
16-07	NARA's Refile Processes at Selected Federal Records Centers	12	The Executive for Agency Services establish standardized policies and procedures for tracking and documenting IRS record problems, including problems with refiles. Identify timeframes for resolution and when the IRS should assist with resolution.
16-07	NARA's Refile Processes at Selected Federal Records Centers	13	The Executive for Agency Services implement a mechanism (database, etc.) to facilitate the problem tracking and resolution process.
16-07	NARA's Refile Processes at Selected Federal Records Centers	14	The Executive for Agency Services identify a resolution for the fifty-six boxes of IRS records maintained in the IRS refile room
16-08	Audit of NARA's FY 2015 Compliance with Improper Payment Requirements	1	The CFO ensure NARA follows OMB Circular A-136 for improper payment reporting and Do Not Pay Initiative reporting.