OFFICE *of* INSPECTOR GENERAL

SEMIANNUAL REPORT *to* CONGRESS

OCTOBER 1, 2016 *to* MARCH 31, 2017

NATIONAL ARCHIVES

FOREWORD

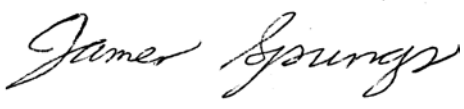
I am pleased to present this Semiannual Report to Congress covering the oversight activities of the Office of Inspector General (OIG) for the National Archives and Records Administration (NARA) from October 1, 2016, to March 31, 2017. Our products continue to assess the effectiveness, efficiency, economy, and integrity of NARA's programs and operations.

During this period a new President was elected, and the new administration has indicated they wish to make the government leaner, accountable, and more efficient. On March 13, 2017, the President issued an Executive order directing the Office of Management and Budget (OMB) to submit a comprehensive plan to reorganize executive branch agencies. As part of this, the head of each agency shall submit to OMB a proposed plan in order to improve the efficiency, effectiveness, and accountability of their respective agency. The audits, investigations, and other products completed by the OIG, and included in this semiannual report, provide NARA with critical information regarding improving efficiency and effectiveness of agency programs and operations. These products identify areas where NARA may realize significant increases in economy and effectiveness, which could lead to cost savings in its operations. This information should serve as a beginning point for management decisions in crafting NARA's plan.

However, unlike most other Federal agencies, NARA will continue to grow and expand due to the nature of its mission. NARA is responsible for identifying, managing, and making available historically significant paper and electronic records from every Federal agency. As history is made every year, NARA's responsibilities and holdings must grow as well. As technology grows and changes each year, NARA's work in storing records made in these new technologies grows and changes as well. NARA faces many significant challenges and obstacles in meeting its mission, the most significant of which are identified in the "NARA Top Ten Challenges" section of this report. During this period the OIG's work continued to point out the difficulty in addressing some of these challenges, now and in the future, due to the growing volume of records and technology advances.

In creating its plan under the Executive order, NARA needs to make an honest assessment of where they can improve to make NARA more efficient and effective. However, NARA must also ensure it adequately communicates the importance of its role and responsibility to the American public, the gravity of the challenges it faces in meeting its mission, and the underlying issue that NARA will only stop growing when the history of this great nation does. NARA must also continue to work with all their stakeholders, such as Congress, to ensure they are fully aware of the challenges and constraints hindering the agency from accomplishing its mission. The OIG stands ready to provide independent oversight and assistance where needed.

I continue to be extremely proud of the hard work and dedication of my staff, and commend their efforts. I also appreciate management's commitment to a strong, independent OIG as shown by their efforts to assist in completion of our work.



James Springs
Inspector General

TABLE OF CONTENTS

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

EXECUTIVE SUMMARY

This is the 57th 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 to 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. Only products labeled as audits are conducted in accordance with the Government Auditing Standards.

Audits of Programs and Operations

- **Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls.** 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 which clearly identifies, prioritizes, and manages risks throughout the organization. Management's internal control activities and assurance statements continue to be based on work at the individual function, program, and office level. This stove-piped focus does not result in all affected offices, programs, and functions evaluating risks that span across the enterprise. Additionally, the Archivist's annual assurance statement to the President and Congress may not clearly reflect NARA's current internal control environment, including risks. (OIG Audit Report No. 17-AUD-01, dated October 28, 2016. See page 13.)

- **Audit of NARA's Compliance with the Federal Managers Financial Integrity Act (FMFIA) for Fiscal Year (FY) 2015.** NARA did not fully develop and maintain effective internal control over its programs and activities, did not sufficiently assess all risks, and did not adhere to all requirements of its own internal control program (ICP). This occurred because NARA lacks complete commitment to internal controls among its managers; full awareness of internal controls and risks across the agency; and resources to develop and maintain an effective ICP. As a result, NARA remains unaware of potential risks and challenges to its programs and activities, and provided its final FY 2015 FMFIA Assurance Statement without adequate, sufficient, and reliable information to support its conclusion. (OIG Audit Report No. 17-AUD-03, dated November 4, 2016. See page 14.)

- **Audit of NARA's Adoption and Management of Cloud Computing.** NARA's approach to cloud computing lacked maturity and adequate planning. The agency moved multiple systems to the cloud without properly considering whether or not the applicable organizations were pragmatically ready. This occurred because NARA lacked a centralized authority with adequate resources to plan and provide the direction necessary. As a result, NARA was not appropriately positioned to fully realize the benefits of cloud

computing and meet OMB's "Cloud First" policy. (Audit Report No. 17-AUD-08, dated March 15, 2017. See page 14.)

- **Audit of NARA's Procurement Program.** NARA lacks effective oversight and management of its acquisition activities. NARA's Procurement Program did not have the proper management support and visibility to adequately align acquisition functions with NARA's mission and needs. Finally, NARA lacks effective controls over its acquisition workforce training and certifications. Without effective organizational alignment and adequate controls, NARA cannot implement a coordinated and strategically oriented approach to its acquisition activities. (OIG Audit Report No. 17-AUD-06, dated November 15, 2016. See page 15.)

- **Audit of NARA's System Inventory.** Information Services does not maintain a comprehensive and accurate information system inventory. We found missing data fields, inaccurate information, and information systems managed by NARA personnel and contractors that were not included on NARA's master systems inventory. This occurred because Information Services has not finalized and implemented systems inventory guidance; has not documented a process for identifying information systems that should be listed on the inventory; and has not clearly defined who is responsible for maintaining the inventory. Federal Law requires the head of each agency to develop and maintain an inventory of the information systems operated by or under the control of such agency. Without a comprehensive and accurate systems inventory, NARA has reduced assurance information systems are adequately acquired/engineered, operated, and maintained to provide acceptable security. (OIG Audit Report No. 17-AUD-02, dated November 4, 2016. See page 16.)

- **Audit of NARA's Management Control Over Microsoft Access Applications and Databases.** We identified 1,800 MS Access applications/databases, and found NARA did not have appropriate operational and security controls in place to ensure uninterrupted functionality and data security for the conversion from MS Access 2007 to 2013. In addition, NARA does not have governing policy for authorizing and approving MS Access applications/databases, and existing policies and procedures for protecting the security and integrity of data have not been adequately implemented. These weaknesses exist primarily because NARA lacks effective management and internal controls. Lack of effective controls jeopardizes NARA's ability to effectively and efficiently carry out critical functions and puts the agency at risk of causing substantial harm, embarrassment, or inconvenience to those whose PII is stored or maintained in its databases. (OIG Audit Report No. 17-AUD-04, dated November 18, 2016. See page 17.)

- **Audit of NARA's Compliance with Homeland Security Presidential Directive 12 (HSPD-12).** NARA did not fully implement all HSPD-12 requirements and missed critical deadlines. In addition, NARA did not develop an agency-wide cost estimate detailing all costs related to implementing HSPD-12, and continued to report unsupported implementation dates to OMB. We attributed these conditions to NARA not prioritizing implementation of the directive, and not having effective management

controls in place to adequately plan and execute requirements. There is an increased risk of redundant expenses, wasted resources, and HSPD-12 goals not being achieved; leaving NARA facilities, networks, and information systems at increased security risk. Also, without an implementation plan, NARA will not be able to establish a reasonable, firm full implementation date. (OIG Audit Report No. 17-AUD-07, dated February 9, 2017. See page 18.)

- **Audit of NARA's FY 2016 Consolidated Financial Statements.** NARA received an unmodified opinion on their financial statements. There was one significant deficiency in internal control over financial reporting related to information technology. There were no material weaknesses in internal control over financial reporting and no instances of noncompliance with certain provisions of laws and regulations. (OIG Audit Report No. 17-AUD-05, dated November 11, 2016. See page 19.)

Other Reports Concerning NARA Programs and Operations

- **Financial Statement Management Letter for FY 2016.** During the audit of NARA's consolidated financial statements as of, and for the year ended, September 30, 2016, the contractor also became aware of various less serious deficiencies in internal control. This is common during financial statement audits and, as in past years, the contractor noted these issues in a Management Letter. This year the issues related to payroll, travel policy, reconciliation between Maximo (NARA's Property System) and the subsidiary ledger, and incorrect allocation of project payments. The Management Letter made four new contractor recommendations, and three contractor recommendations from prior years were closed. (OIG Letter dated November 10, 2016. See page 20.)

- **Narrative Report on NARA's FY 2016 Federal Information Security Management Act (FISMA) Compliance.** NARA made significant efforts in the area of Security and Privacy Training to address some weaknesses identified in previous FISMA evaluations and audit engagements. As a result, we determined NARA's overall security and privacy training program was effective for this assessment period. However, we found NARA still needs significant improvement in seven of the eight metric domains in order to be consistent with FISMA and National Institute of Standards and Technology (NIST) guidance. Many of the weaknesses identified pertained to underdeveloped and inconsistently implemented policies and procedures. (OIG Report No. 17-R-07, dated November 9, 2016. See page 20.)

- **Follow-up on NARA's Preparation for the Receipt of President Obama's Administration's Electronic Records.** The OIG advised the Archivist of our concerns about the Electronic Records Archives (ERA) Executive Office of the President (EOP) System's ability to adequately handle the electronic records from President Obama's administration. Specifically, at the time none of the administration's electronic records had been indexed into the ERA EOP System, nor had a contingency plan been adequately developed or implemented. This could potentially result in significantly longer response times to special access requests. (OIG Report No. 17-ML-10, dated December 19, 2016. See page 21.)

- **Researcher Issues on Accessing and Using Partner-Digitized Records.** NARA works with various non-Federal partners to have the partner digitize NARA holdings. In exchange, among other things, these entities are generally to provide free access to the images from NARA computers. NARA then does not serve the original to researchers unless there is some compelling special reason. In an extremely limited spot check of how staff presented partner digitized records to researchers at NARA's College Park, MD facility we found the research room computers had no directions or instructions, and NARA's website was potentially confusing and may unnecessarily lead researchers to pay-for-use websites. Further, the records may be presented with copyright markings and be subject to use restrictions in partners' non-intuitive website terms and conditions. (OIG Report No. 17-ML-11, dated March 10, 2017. See page 22.)

- **Purchase and Travel Card Risk Assessment.** Under the requirements of the Government Charge Card Abuse Prevention Act of 2012 we performed an assessment of NARA's Charge Card Program. NARA's risks remain at a moderate level. While some issues remain, in general NARA's policies and procedures are designed to provide reasonable assurance for implementing and managing the NARA Charge Card Program and to mitigate the potential for fraud, misuse, and delinquency. (OIG Memorandum dated February 7, 2017. See page 22.)

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.

- Continued running the Whistleblower Ombudsman program, providing training and information to potential whistleblowers on various rules and protections available. This work included one-on-one consultations with individuals and meeting with the Senate Whistleblower Caucus.
- 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.
- Provided suggestions on improving NARA 1572: Preventing Theft and Vandalism of NARA Holdings in NARA Facilities, including how research room staff are to react when they witness criminal activity and how access is granted to specially protected holdings areas.
- Provided comment and input into several other NARA directives and regulations covering a variety of topics.
- Provided NARA with a Presidential transition landing team information sheet on the OIG and our concerns.
- Responded to over 21 requests from NARA for reviews of proposed legislation, Office of Management and Budget (OMB) regulations, congressional testimony, and other items.
- An OIG-specific logo was created with NARA design professionals.

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 conduct assessments of areas with the potential for fraud, or issue management letters detailing specific issues or vulnerabilities we observe. Assessments are typically not designed to be in-depth, detailed accounts, and are used to alert management to issues. Accordingly, they do not follow any set standards or procedures.

In this period the OI received and reviewed 173 complaints and other intake actions, opened 18 new investigations, and closed 10 existing investigations. Local authorities accepted the one person referred for potential criminal prosecution.

Highlights for this reporting period include:

- 75 percent of our closed or completed investigations resulted in referrals for criminal, civil, and/or administrative action.
- OI agents recovered two historically significant Leavenworth Federal Penitentiary inmate photographs which were stolen over a decade ago. The photographs depict Native Americans, Mary Snowden and Henry Shemany.
- OI agents recovered 10 alienated United States Navy submarine blueprints.
- OI agents conducted five investigations involving senior NARA officials.
- Approximately 33 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.

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 records in its custody and control. Public access to these records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history in order to participate more effectively in 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 over five 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 685,000 artifacts and approximately 710 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 fiscal year (FY) 2016, NARA had over 85 million online visits in addition to hosting 4.3 million traditional visitors, all while responding to more than 1.1 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 14 Presidential libraries preserving the papers and other historical materials of all past Presidents since Herbert Hoover.

Resources

During this reporting period NARA operated under a continuing resolution funding NARA at FY 2016 levels minus a small rescission, and providing an additional $4.85 million for the Presidential Transition. In FY 2016, NARA was appropriated $389 million, including $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 2,856 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

Just as NARA, in this period the OIG operated under a continuing resolution funding the office at FY 2016 levels minus a small rescission. In FY 2016, Congress provided $4.18 million for the OIG's appropriation, including authorization for 24 FTEs. During this period selections were made for the Assistant Inspector General for Audits (AIGA) and the Assistant Inspector General for Investigations (AIGI) positions. Further, a new administrative assistant was hired. Currently the OIG has 19 FTEs on board, including an Inspector General, nine FTEs devoted to audits, seven FTEs devoted to investigations, an administrative assistant, and a counsel to the Inspector General.

Involvement in the Inspector General Community

Council of Inspectors General on Integrity and Efficiency (CIGIE)

CIGIE is an independent entity within the executive branch created to address integrity, economy, and effectiveness issues that transcend individual agencies and aid in establishing a professional, well-trained, and highly skilled workforce in the Federal OIGs. The Inspector General is a CIGIE member, and regularly attends meetings discussing government-wide issues and congressional items affecting the Inspector General community.

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 CIGIE's legislative priorities; answering various data calls; monitoring legislation for developments of interest to the community; and developing input for proposed legislative actions. During this reporting period the committee was active with the final development and passage of the Inspector General Enhancement Act of 2016, a landmark piece of legislation welcomed by CIGIE.

CIGIE Audit Committee

The Audit Committee provides leadership to, and serves as a resource for, the Federal IG 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 gives 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 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 Investigations Committee in the performance of its duties.

Council of Counsels to Inspectors General (CCIG)

The OIG counsel currently serves as a vice chair 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 from across the Federal community. Through the CCIG, counsel also began work with a team tasked to develop a new course

designed to give new OIG attorneys the community specific information and foundation they will need.

CIGIE Training Institute

The OIG counsel continued to work with the CIGIE Training Institute. In this period OIG counsel worked closely with other instructors and CIGIE staff to completely revise and update the structure, presentation, and content of the Inspector General Authorities course. Further, counsel is working with the Training Institute on developing a course for new IGs.

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 recently peer reviewed by the National Labor Relations Board (NRLB) 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. NRLB OIG concluded "the system of quality control for the audit organization of the NARA OIG, in effect for the 12-months ended September 30, 2016, 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 no 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 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.

NARA OIG Peer Review of Other OIGs

The NARA OIG did not conduct a peer review of any other OIGs during the reporting period, and there are no recommendations from previous peer reviews that remain outstanding or have not been fully implemented. Our Office of Audits is scheduled to conduct a peer review of the Export-Import Bank of the United States for the period ending March 31, 2017.

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 OIG Budgets

The OIG responded to an information request from the Senate Homeland Security and Government Affairs Committee concerning historical budget information.

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.

Constituent Complaint Concerning NARA Staff

The OIG responded to a Senator's office concerning questions about a constituent's complaint. The constituent requested confirmation the OIG had received their complaint that they were treated inappropriately by NARA staff in a research room.

Audit and Reports Overview

During this reporting period, the OIG issued eight final audits, and five other reports. These other reports include such things as Management Letters (which are less detailed alerts to management about issues which should not wait for, or do not warrant, an actual audit) and do not follow the Government Auditing Standards. 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.

Additionally, we initiated or continued work on the following audits or other non-audit reports:

- Audit of NARA's Freedom of Information Act (FOIA) Process – to determine whether NARA's FOIA process is efficient, effective, and complies with current laws and regulations; and assess whether internal controls are in place to ensure NARA responds to FOIA requests timely and accurately.
- Audit of NARA's Electronic Records Archive (ERA) System 2.0 – to evaluate and report on the current status of the ERA 2.0 development effort.
- Audit of NARA's Online Access to Digitized Holdings – to evaluate NARA's controls in place to achieve its Strategic Goal of "Make Access Happen" by providing online access to its digitized holdings through the National Archives Catalog.
- Audit of NARA's FY 2016 compliance with Improper Payment Requirements – to determine NARA's compliance with improper payment requirements based on OMB Memorandum 15-02 and OMB Circular A-136.
- NARA's Compliance with the Digital Accountability and Transparency (DATA) Act – to assess NARA's readiness to implement the provisions of the DATA Act of 2014.
- CIGIE's Cross-Cutting Purchase Card Project/Audit of the Travel and Purchase Cards Programs – to determine whether internal controls for NARA's Purchase Card Program (PCP) are adequately designed and appropriately implemented to effectively deter fraud, waste, or abuse; the PCP has effective oversight and management; and the PCP is operating in compliance with applicable laws, regulations, and agency policies.
- Office of the Federal Register's Administration of the Electoral College Process – to determine whether the Office of the Federal Register implemented proper controls for the administration of the Electoral College process, including properly maintaining records.
- Audit of NARA's Human Capital Practices – to determine whether NARA's human capital practices are operating efficiently and effectively.
- Audit of NARA's Continuity of Operations Readiness – to determine whether NARA has appropriate processes and controls in place to continue its mission-essential functions with minimal disruption in case of a contingency.

Audit Summaries

Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls

The Federal Managers' Financial Integrity Act, Public Law 97-255, requires each agency to establish controls that reasonably ensure:

- obligations and costs comply with applicable law,
- assets are safeguarded against waste, loss, unauthorized use or misappropriation, and
- revenues and expenditures are properly recorded and accounted for.

The Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, defines management's responsibility for internal control and the process for assessing internal control effectiveness in Federal agencies. It provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control.

While NARA appeared to be aware of the significant risks and challenges they face, NARA did not fully implement an Enterprise Risk Management (ERM) program that clearly identified, prioritized, and managed risks throughout the organization. We noted NARA management did not make the implementation of an ERM program a strategic priority and instead has been relying on its Internal Control Program (ICP) and Management Control Oversight Council to identify and manage risks throughout the organization. As a result, NARA's internal control activities and assurance statements continued to be based on work at the individual function, program, and office level. As a result of this stove-piped focus, risks that spanned across the enterprise were not being evaluated by all affected offices, programs, and functions to ensure the risks within each office were at an acceptable level. Enterprise-wide risks include things such as risks related to information security, hiring, and the allocation of limited resources. Without an effective ERM process in place that clearly identifies, categorizes, and assesses the effectiveness of controls related to key risks, the Archivist's annual assurance statement to the President and Congress may not clearly reflect NARA's current internal control environment, including risks.

Additionally, while NARA implemented an ICP, we noted its implementation of the program needed improvement. Specifically, requirements outlined in NARA's existing ICP policies and procedures were not consistently followed by the offices and programs responsible for completing ICP activities. Additionally, NARA's lack of an ERM program meant risks identified during the ICP process were not formally aligned to NARA's strategic goals and objectives. This occurred primarily due to a lack of formal training and oversight of all ICP activities being carried out NARA offices and programs. NARA's weaknesses with its ICP mean it was not realizing important benefits of an effective ICP, including:

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

The report makes eight recommendations to strengthen NARA's internal control environment and provide senior management with greater assurance that management's conclusions in their formal assurance statements are accurate. It also included five suggestions to help management improve their controls over high-risk areas within the organization. (OIG Audit Report No. 17-AUD-01, dated October 28, 2016.)

Audit of NARA's Compliance with the Federal Managers Financial Integrity Act (FMFIA) for FY 2015

The annual FMFIA Assurance Statement represents the agency head's informed judgment as to the overall adequacy and effectiveness of internal control within the agency. Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control (Circular A-123), emphasizes the need for integrated and coordinated internal control assessments that synchronize all internal control-related activities. We audited the National Archives and Records Administration's (NARA) compliance with Circular A-123, FMFIA, and internal guidance related to internal controls. We also evaluated the system of internal controls for NARA program offices, the accuracy of NARA's FY 2015 FMFIA Assurance Statement, and supporting individual office assurance statements.

We found NARA did not fully develop and maintain effective internal control over its programs and activities, did not sufficiently assess all risks, and did not adhere to all requirements of its own ICP. This condition occurred because NARA lacks complete commitment to internal controls among its managers; full awareness of internal controls and risks across the agency; and resources to develop and maintain an effective ICP. As a result, NARA remains unaware of potential risks and challenges to its programs and activities, and it provided its final FY 2015 FMFIA Assurance Statement without adequate, sufficient, and reliable information to support its conclusion.

The report makes 10 recommendations to initiate improvements which, when implemented, will strengthen NARA's ICP. The opportunity also exists for NARA to greatly improve its ICP by reviewing and adhering to the recent revision to Circular A-123, and addressing and implementing prior year audit recommendations. (OIG Audit Report No. 17-AUD-03, dated November 4, 2016.)

Audit of NARA's Adoption and Management of Cloud Computing

OMB directed agencies to shift to a "Cloud First" policy on December 9, 2010. NARA reported moving services to the cloud as early as 2011 and, like other Federal agencies, continues to evaluate existing and new services for cloud computing opportunities, increasing spending on cloud computing annually.

However, NARA's approach to cloud computing lacked maturity and adequate planning. We found NARA moved multiple systems to the cloud without properly considering whether or not the applicable organizations were pragmatically ready to migrate services to the cloud. This occurred because NARA lacked a centralized authority point with adequate resources to conduct

the planning and provide the direction necessary for NARA's transition to cloud computing. As a result, NARA was not appropriately positioned to fully realize the benefits of cloud computing and meet OMB's "Cloud First" policy.

NARA lacked an accurate cloud computing inventory. NARA maintained several differing inventory listings and had not established an effective method to accurately inventory its cloud computing services. This occurred because NARA lacked a common identifier and designation for its cloud computing services, and did not use a centralized reporting point for those services. As a result, it will be difficult for NARA to apply the controls needed for the unique environment of cloud computing. This will also impair NARA's ability to accurately report performance information related to its cloud computing activities.

NARA also executed cloud contracts without established standards in place. Despite years of implementing cloud computing contracts, NARA did not yet have an approved requirement to include a common set of procedures for CSPs to follow, including expected levels of service, as part of its cloud computing contracts. No reviews were conducted to determine the extent of contracts that may be without Service Level Agreements (SLAs). In addition, NARA's approach to monitoring cloud contracts lacked a central location for maintaining reports. Further, NARA was executing its cloud computing contracts without approved standards for contractual language. NARA did not consider development of cloud provisioning guidelines a priority, which may have impaired NARA's ability to establish effective controls and monitor service levels of cloud computing contracts. As a result, NARA may not be able to consistently and accurately measure the performance levels of NARA's cloud computing contracts in order to achieve the full benefits of a "Cloud First" policy.

Additionally, the Capital Planning and Investment Control's (CPIC's) Business Case Form could be improved. The design and content of CPIC's Business Case Form did not allow for consistent and comprehensive collection of information needed for proposed IT investments. This occurred because CPIC did not incorporate relevant guidance and best practices for IT acquisitions into the content of the form. The form used lacked formal approval and was part of a temporary directive for interim guidance from FY 2013 (NARA 801-3, Temporary Capital Planning and Investment Control Process, September 17, 2014). As a result, CPIC's Business Case Form was not as effective as it could be at capturing beneficial information on NARA's cloud computing activities. This may impair NARA's ability to make decisions which ensure IT projects align with NARA's mission and strategic goals.

NARA may not be fully considering the benefits of FedRAMP's "do once, use many times" approach. NARA needs to develop and implement a standard and comprehensive approach to its cloud computing activities and coordinate processes across business lines. We made 10 recommendations, which are intended to improve the performance of NARA's cloud computing program. (OIG Audit Report No. 17-AUD-08, dated March 15, 2017.)

Audit of NARA's Procurement Program

Effective organizational alignment, coupled with strong leadership, enables organizations to implement a coordinated and strategically oriented approach to acquisition activities. The

quality and effectiveness of the Federal acquisition process depends on developing a capable and competent workforce, and implementing strong internal controls. We performed this audit to assess the effectiveness and efficiency of NARA's procurement program in acquiring goods and services.

NARA's Procurement Program did not have the proper management support and visibility within the organization to adequately align acquisition functions with NARA's mission and needs. NARA's acquisition function is not adequately aligned with leadership, key procurement executives are not designated, and required duties and responsibilities are not carried out. NARA has not made procurement a strategic priority and has not assigned its acquisition functions the proper degree of responsibility and authority for strategic planning. Without effective organizational alignment and strong leadership, NARA cannot implement a coordinated and strategically oriented approach to its acquisition activities to ensure mission needs are met.

NARA lacks effective oversight and management of its acquisition activities. NARA's contract oversight office is not staffed, evaluations of internal controls are ineffective and inconsistent, policies and procedures are not up to date, contract files are missing key documents, contracts are not awarded in a timely manner, and the acquisition workload is not proportionate to staff levels. We attribute these conditions to ineffective management decisions and inadequate monitoring of internal controls. When monitoring is not designed and implemented appropriately, organizations are less likely to identify and correct internal control problems on a timely basis.

In addition, NARA lacks effective controls over its acquisition workforce training and certifications. Contracting personnel are not trained commensurate with warrant authority or Contracting Officer Representative oversight levels, training is not adequately tracked, and program and project management certifications are not properly approved. NARA management is not providing the level of oversight required to ensure appropriate training is occurring. Without adequate training and oversight, NARA cannot ensure its acquisition workforce has the competencies necessary to adequately identify needs, develop requirements, perform contracting and purchasing, and oversee contracts for the agency.

We recommended NARA give critical attention to strengthening internal controls over acquisition functions and provide better oversight and management of its procurement activities to ensure effective and efficient processes and procedures that adhere to Federal and internal guidance. This report includes 26 recommendations intended to strengthen the management, accountability, and oversight of NARA's Procurement Program. We intend to conduct follow-on reviews of procurement areas identified during this audit. (OIG Audit Report No. 17-AUD-06, dated November 11, 2016.)

Audit of NARA's System Inventory

Information system inventories are the basic tools used by agencies to support information resource management processes including information technology planning, budgeting, acquisition, monitoring, testing, and evaluation of information security controls. A key goal of the inventory process is to ensure information systems are acquired/engineered, operated, and

maintained to provide acceptable security. We performed this audit to determine if NARA has developed a comprehensive information system inventory to track and monitor all information systems operated or maintained throughout the agency. We also evaluated NARA's information systems to determine if they were adequately classified and categorized.

Information Services does not maintain a comprehensive and accurate information system inventory. We found missing data fields, inaccurate information, and information systems managed by NARA personnel and contractors that were not included on NARA's master systems inventory. This occurred because Information Services has not finalized and implemented systems inventory guidance; has not documented a process for identifying information systems that should be listed on the inventory; and has not clearly defined who within Information Services is responsible for maintaining the information system inventory. Federal law requires the head of each agency to develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency. Without a comprehensive and accurate systems inventory, NARA has reduced assurance its information systems are adequately acquired/engineered, operated, and maintained to provide acceptable security.

In addition, NARA system owners were not adequately categorizing information systems using Federal Information Processing Standards Publication 199 (FIPS 199). Controls were not in place to ensure system owners used proper documentation to categorize the systems. System owners were either using incomplete FIPS 199 categorization documentation provided by Information Services or not using FIPS 199 at all to categorize their information system. Incorrect FIPS 199 security categorization can result in the agency either over-protecting the information system thus wasting valuable security resources, or under-protecting the information system and placing important operations and assets at risk. Consequently, NARA may not be providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

We recommended NARA develop, document, approve, and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c), and comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are accurately categorized. (OIG Audit Report No. 17-AUD-02, dated November 4, 2016.)

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

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

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

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

Additionally, during the audit, a database was deleted from the server by a NARA employee after the OIG requested supporting documentation on it. Although we determined the deletion was not due to a concealment of a fraud or employee misconduct, the deletion raised concern about employees' awareness of their responsibility to cooperate with OIG audit requests and abide by NARA's Records Schedule.

We recommended NARA evaluate the MS Access applications and databases used in each program office to determine their data sensitivity and mission-criticality, implement the security assessment process in accordance with their data sensitivity and mission-criticality, and develop a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system. We made nine recommendations which, if implemented, will assist NARA in adequately preparing for its planned Microsoft Access upgrade. (OIG Audit Report No. 17-AUD-04, dated November 18, 2016.)

Audit of NARA's Compliance with Homeland Security Presidential Directive 12

Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004, directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. OMB issued a Memorandum, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (M-05-24), providing implementing instructions for Federal agencies for HSPD-12 and Federal Information Processing Standard 201. The standard identification

applies to employees and contractors who work at an agency's facilities or have access to an agency's information systems.

The objective of this audit was to determine whether NARA effectively complied with HSPD-12 requirements for accessing NARA facilities and information systems. The audit was conducted at the National Archives Building (Archives I) and the National Archives in College Park, MD (Archives II).

We found although NARA had already spent approximately $2.8 million and utilized many resources, HSPD-12 requirements were not fully implemented and critical deadlines were missed. Specifically, NARA did not (1) complete an implementation plan, (2) develop and issue an HSPD-12 implementation policy, and (3) formally designate an agency lead official for ensuring issuance of the agency's HSPD-12 implementation policy. In addition, NARA did not develop an agency-wide cost estimate detailing all costs related to implementing HSPD-12, and continued to report unsupported implementation dates to OMB. We attribute these conditions to NARA not making implementation of the directive a priority and not having effective management controls in place to adequately plan and execute requirements to ensure full and timely implementation of HSPD-12. Without adequate management controls and an agency-wide approach for documenting and monitoring expenses, there is an increased risk of redundant expenses, wasted resources, and HSPD-12 goals not being achieved, leaving NARA facilities and information systems at increased security risk. We made four recommendations to improve NARA's efforts in implementing HSPD-12. (OIG Audit Report No. 17-AUD-07, dated February 9, 2017.)

Audit of NARA's Fiscal Year 2016 Consolidated Financial Statements

We contracted with CliftonLarsonAllen LLP (CLA), a public accounting firm, to audit NARA's Consolidated Balance Sheets as of September 30, 2016; and the related Statements of Net Cost, Changes in Net Position, and Budgetary Resources.

NARA received an unmodified opinion on it's FY 2016 financial statements. CLA reported one significant deficiency in internal control over financial reporting related to information technology. CLA disclosed no material weaknesses or instances of noncompliance with certain provisions of laws and regulations. There was one recommendation.

We monitored CLA to ensure the audit was conducted in accordance with the contract, and in compliance with the Government Accountability Office's Government Auditing Standards and other authoritative references, such as OMB Bulletin No. 15-02, Audit Requirements for Federal Financial Statements. Our review disclosed no instances wherein CLA did not comply, in all material respects, with the contract or Government Auditing Standards. (OIG Audit Report No. 17-AUD-05, dated November 11, 2016.)

Summaries of Other Major Reports

Fiscal Year 2016 Financial Statement Management Letter

During our audit of NARA's consolidated financial statements as of and for the year ended September 30, 2016, our contractor, CLA also became aware of deficiencies in internal control other than significant deficiencies and material weaknesses and other matters that represent opportunities for strengthening internal control and operating efficiency. While the nature and magnitude of these other deficiencies in internal control were not considered important enough to merit the attention of those charged with governance, they are considered of sufficient importance to merit management's attention. Management Letter comments related to payroll, travel policy, reconciliation between Maximo (NARA's Property System) and the subsidiary ledger, and incorrect allocation of project payments. These were issues which did not rise to the level of a formal audit recommendation, and were provided to NARA for consideration only. The OIG does not track these contractor recommendations. CLA made four contractor recommendations in the Management Letter, and three contractor recommendations from prior years were closed. (OIG Letter dated November 10, 2016.)

Narrative Report on NARA's FY 2016 Federal Information Security Management Act (FISMA) Compliance

Each year the Federal Information Security Modernization Act of 2014 (FISMA) requires an independent evaluation of NARA to determine the effectiveness of its information security practices. We completed our evaluation in accordance with FISMA, OMB Memorandum M-16-03, and Department of Homeland Security (DHS) FY 2016 Inspector General FISMA Reporting Metrics, which provided the reporting instructions for meeting FISMA requirements.

Our evaluation found NARA made significant efforts in the area of Security and Privacy Training to address some weaknesses identified in previous FISMA evaluations and audit engagements. Examples of some of these efforts include, and are not limited to the following.

- Designation of Information System Security Officers (ISSOs) to perform security support services;
- Identification of individuals with elevated security responsibilities for Tier-II security and privacy awareness training and the Logical Access Control System (LACS);
- Progress with the implementation of HSPD-12;
- Development and deployment of Tier-II security and privacy awareness training and the insider threat program.

As a result of NARA's efforts in this metric domain, we determined NARA's overall security and privacy training program was effective for this assessment period. However, we found NARA still needs significant improvement in seven of the eight metric domains in order to be consistent with FISMA and National Institute of Standards and Technology (NIST) guidance. Many of the weaknesses identified from the seven metric domains pertained to underdeveloped and inconsistently implemented policies and procedures, which potentially expose the

confidentiality, integrity, and availability of the agency's information and information systems to unauthorized access, use, disclosure, disruption, modification, or destruction.

Although NARA made progress in its information security program by designating ISSOs in FY 2016, the ISSOs arrived too late in the fiscal year to make any significant impact in this reporting period. The ISSOs are in charge of ensuring compliance with NIST guidance and NARA policy for their assigned systems. Therefore, we expect further improvement to NARA's information security in the next reporting period and years to come. (OIG Report No. 17-R-07, dated November 11, 2016.)

Follow-up on NARA's Preparation for the Receipt of President Obama's Administration's Electronic Records

The OIG advised the Archivist of our concerns about the Electronic Records Archives (ERA) Executive Office of the President (EOP) System's ability to adequately handle the electronic records from President Obama's administration. Specifically, none of the administration's electronic records have been indexed into the ERA EOP System, nor has a contingency plan been adequately developed or implemented. This could potentially result in significantly longer response times to special access requests than during the last two change in administrations.

On January 20, 2017, legal custody of the records from President Barack Obama's administration transferred to 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. Such public access does not commence until five years after the President leaves office. In addition, NARA strives to be able to respond to time-sensitive and often high-visibility special access requests for these records, which come from former and incumbent Presidents, the courts, and the Congress, as soon as possible after the President leaves office. Providing such access, however, must be consistent with the Archivist's responsibility for assuming "the custody, control, and preservation of" the Presidential records.

Since the issuance of OIG Report Number 16-06 entitled NARA's Preparation and Planning for the Receipt of President Obama's Administration's Records and Artifacts on May 6, 2016, we continued to follow up and monitor the transfer of electronic records from the EOP to NARA. On November 15, 2016, we requested the number of EOP electronic records that have been copied, ingested, and indexed in the ERA EOP System. On November 22, 2016 we received a response stating 308,816,606 files were under archival control in the Data Transport Hardware and Software (DATR), i.e., copied and ingested. In addition, we were told indexing is underway. However, we could not reconcile these numbers to the weekly dashboard for this project at that time, nor could we reconcile to the DATR Status as of December 8, 2016, almost three weeks later. The numbers on December 8th showed 306,490,141 records in the DATR and no records indexed. During the ERA EOP System upgrade, it took the contractor almost four months to

index the EOP George W. Bush data, which was about one-third of the size of the anticipated electronic records from President Obama's administration.

NARA has always strived to make the EOP high-priority records available as soon as possible after the Presidential transition. For example, after the Clinton and Bush transitions, NARA had many of the high-priority records searchable within hours of taking legal custody. During the Bush transition, the data in the ERA EOP System was not indexed until September 2009, eight months after inauguration day. However, this did not prevent NARA from responding to special access requests in a timely manner. By implementing a contingency plan that allowed NARA to take custody of the EOP's systems deemed to be high priority, NARA officials were able to respond to these requests by performing searches on those applications until the data in the ERA EOP System was indexed and searchable.

NARA officials never developed any trigger conditions, nor does it appear they have any intention of invoking a contingency plan. Without any trigger conditions or an adequate contingency plan in place, it appears NARA's plan to address special access requests will be to rely solely on the ERA EOP System. However, the current schedule shows the Authority to Operate (ATO) this system is not planned until April 2017. This potentially could mean the response times for special access requests will be measured in terms of months, instead of hours or days. This could also result in embarrassment to the agency if responses to special access requestors are not fulfilled as timely as they were during the last two changes in administrations. We continue to believe a contingency plan is needed in order to respond timely to special access requests received prior to the ATO being issued for the ERA EOP System. Therefore, NARA should review any alternative options that could be used. (OIG Report No. 17-ML-10, dated December 19, 2016.)

Researcher Issues on Accessing and Using Partner-Digitized Records

In response to a complaint, the OIG conducted an extremely limited review of how a record scanned by a private partner would be presented to a researcher at NARA's College Park, MD facility. NARA generally does not serve original records to researchers once they are scanned. Instead, under the terms of the digitization agreements, NARA researchers can access the digitized images free of charge on the partner's website using computers at NARA facilities.

The research room computers had no directions or instructions, and the NARA website was potentially confusing which may unnecessarily lead researchers to pay-for-use websites. Further, once located, the records may appear to have copyright markings and be subject to use restrictions in partners' non-intuitive terms and conditions. (OIG Report No. 17-ML-11, dated March 10, 2017.)

Purchase and Travel Card Risk Assessment

The Government Charge Card Abuse Prevention Act of 2012 (the Act) requires the Inspector General of each executive agency to conduct, at minimum, annual assessments of the agency's purchase card program and to perform analysis or audits, as necessary, of purchase card transactions.

We performed an assessment of NARA's Charge Card Program and reported the results to the head of the agency. NARA's purchase and travel card risks remain at a moderate level. In general, NARA's policies and procedures are designed to provide reasonable assurance for implementing and managing the NARA Charge Card Program and to mitigate the potential for fraud, misuse, and delinquency. However, there remain several open recommendations from previous audits that have not yet been addressed. We have started an audit of the agency's Purchase Card Program. We also plan to audit Purchase and Travel Card Programs or certain aspects of the programs on a recurring basis (every three years) to assess program efficacy and oversight. (OIG Memorandum dated February 7, 2017.)

The Act also requires Inspectors General report to the Director OMB annually on agency progress in implementing audit recommendations. On January 31, 2017 we sent OMB a memorandum on six outstanding recommendations from three OIG audit reports related to NARA charge cards:

- OIG Audit Report No. 08-02, Audit of NARAs Purchase Card Program;
- OIG Audit Report No. 11-14, Audit of Foreign and Premium Travel; and
- OIG Audit Report No. 16-05, Audit of NARA's Public Facing Websites.

However, on March 14, 2017, two outstanding recommendations relating to OIG Audit Report #11-14, Audit of Foreign and Premium Travel, were closed.

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 alert management to potential problems or vulnerabilities through Management Letters or other products if a full investigation is not warranted or appropriate. The OI may also conduct assessments of areas with the potential for fraud. Assessments are typically designed to proactively look into aspects of NARA's programs and operations such as contract compliance and telework adherence. They are intended to be quick looks at potential issues, and are not designed to be in-depth, detailed accounts. Accordingly, they do not follow any set standards or procedures. The purpose is to alert management to issues. While they may offer suggestions, they generally do not make recommendations for corrective action.

Significant Investigations and Updates

Veteran Falsifies Records for Federal Benefits

Previously we reported a veteran had obtained personal military records from NARA and fraudulently altered them show he had overseas military service during the time his properties were foreclosed. The purpose of this fraudulent alteration was to obtain relief under the Servicemembers' Civil Relief Act as the victim of an unlawful foreclosure of those properties while he was serving overseas. Had the fraud been successful, the veteran could have collected approximately $730,000. Following a June 2016 plea of "guilty" to one charge of making a false statement, in January 2017 the subject was sentenced to six months in prison followed by two years of supervised release.

Time and Attendance Abuse

We received an allegation that a NARA employee had committed time and attendance fraud, and their supervisor, a friend, was complicit. The investigation substantiated that, during a two-month period in 2015, the employee knowingly entered false information into a Form 3032B Daily Time and Attendance Record. The investigation did not substantiate the allegation that the supervisor was complicit. However, it did show that the supervisor had been negligent with respect to oversight, particularly given that the employee's time and attendance record-keeping had been called into question before. The matter was presented to the Office of the United States Attorney, but criminal prosecution was declined in favor of administrative action. In this reporting period, the employee received a 14-day suspension, and the supervisor received a 2-day suspension.

Unauthorized Secondary Employment at the Workplace

We received an allegation that a NARA employee had engaged in unauthorized secondary employment in the workplace selling merchandise. The investigation determined that the employee was not employed by the merchandise company. However, the NARA employee had acted informally on behalf of a friend, and had engaged in several activities in the workplace in

order to help their friend sell merchandise. In this reporting period, the employee received a three day suspension.

Misuse of Information Technology Equipment

Working from raw data pertaining to information technology (IT) usage by NARA employees in the workplace, we developed an investigation of a NARA employee who had spent significant fractions of their workdays using NARA IT equipment to download video games and stream music. Between May 2015 and May 2016, the employee was determined to have spent half or more of their working hours engaged in this misconduct almost every day, and to have accounted for a large amount of all bandwidth usage by all NARA employees. The employee had also installed an unauthorized software program on their NARA-issued IT equipment. In this reporting period, the technician served a one-day suspension for the violation.

Leavenworth Federal Penitentiary Inmate Photographs Recovered for NARA

Previously we reported that Leavenworth Federal Penitentiary inmate photographs that should have been part of NARA's holdings were instead available for sale on eBay. As the result of extensive coordination both with the dealer and with people who had already purchased some of the photographs, we were initially able to recover 42 of the 57 photographs. Since our last report, NARA has recovered another two of the missing original photographs, those pertaining to inmates Mary Snowden and Henry Shemany.

Recovery of Non-Accessioned United States Navy Submarine Blueprints

NARA requested assistance from the OI in recovering Navy submarine blueprints that were potentially stolen and sold by a private citizen online. The OI subpoenaed the seller and contacted parties. It was determined the blueprints should have been part of NARA's holdings, but had never actually been accessioned into NARA. The OI recovered 10 of the blueprints that should have been accessioned at NARA. Information was provided to NARA for NARA to determine further action on additional documents.

Misuse of Information Technology Equipment

Working from raw IT usage data by NARA employees in the workplace, we developed an investigation of an employee who had used NARA IT equipment to download significant quantities of pornographic still images and videos from at least April 2014 to the investigation date. Presented with a notice of intention for a 14-day suspension, the employee instead retired from Federal service in this reporting period.

Arrest Warrant Issued for Contractor Who Threatened Supervisor

In January 2017 the Division of Security Management shared information with the OIG that a former employee of a contractor had been barred from NARA facilities. Following termination, the ex-employee made threatening telephone calls to their former direct supervisor, including a text message and photograph showing the ex-employee surrounded by weapons and wielding a rifle. In this reporting period, our investigation resulted in the issuance of an arrest warrant for the ex-employee. The court hearing was originally scheduled for March 2017, but was postponed to April 2017.

Significant Referrals

Hatch Act Violations During Election Season

Working from a fixed list of specific search terms associated with the national election season, the OI proactively conducted a series of reviews of all NARA employee emails for potential violations of the Hatch Act. The Hatch Act is a Federal law which primarily regulates political activity among Federal executive branch employees. With an initial aggregate return of 4.6 million electronic mail messages, we were able to reduce the overwhelmingly vast majority of the initial returns to a manageable listing of solid potential violations. The OI has coordinated its efforts with the Office of Special Counsel (OSC), which bears primary responsibility for Hatch Act enforcement, and in this reporting period made an official referral of its findings regarding NARA employees who we believed to have committed Hatch Act violations. The OSC accepted the referrals and will determine the next appropriate actions.

Sexual Harassment

We received an allegation that a NARA employee had escalated long-term sexual harassment of a contractor to such an extent that the contractor felt threatened and compelled to report the abuse, despite having reported once previously without effect. The contractor's initial report had been made to a person who was not the NARA employee's supervisor, and the complaint was neither acted-on nor passed-on to an appropriate authority. After conducting initial interviews to address the part of the allegation pertaining to the possibility of an actual threat, the OI referred the matter to the NARA Equal Employment Opportunity Office for action on the sexual harassment element. The agency took quick action and determined both that the NARA employee had violated NARA's policies against harassment, and the person to whom the contractor had initially reported the harassment had failed to pass the matter to the right authorities. In this reporting period, both NARA employees were issued Letters of Reprimand, and were required to re-train with, and to pass, NARA's online anti-harassment training modules. Moreover, the harasser is barred from all future contact with the contractor.

Investigations of Senior Government Employees

Allegations of Potential Conflict of Interest

The OI received an anonymous allegation that the subject hired as a direct subordinate a person who was also their partner in a company in which both had ownership interest. Our investigation substantiated that the two were co-owners of company, and clarified that the subject arranged to have the other party, who was already a NARA employee, transferred into the subject's division as a subordinate. The circumstances of the transfer were such that it was not necessary to post a vacancy announcement, nor did the subject do so. The subject did not report the situation to their supervisor, and did not seek guidance from the Office of the General Counsel (OGC) until after the investigation was already ongoing. In response to the OGC's findings, the subject went on unpaid leave from their company. The OI investigation did not establish any actual conflict of interest, or misuse of NARA resources, and reported its findings to the agency in a Report of Investigation. The results of this are anticipated to be reported in the next period.

Allegations of Pre-selecting an Applicant for an Open Position

The OI received an allegation that the subject was involved in the creation of a position description for an unlawfully pre-selected employee. The employee identified as having been "pre-selected" for the position was, in fact, ultimately awarded the position. Our investigation showed the employee had been competently doing the position's work for some time, the hiring process was followed, multiple people applied for the position, and the selected employee was identified as being the most qualified. The allegations were not substantiated.

Allegations of Unapproved Outside Employment

During the course of an unrelated investigation, the OI developed information indicating that a subject operated a catering business from their residence on days designated as telework days from NARA. Our investigation established that the subject does operate a catering business from their residence, but the appropriate permissions had been obtained, and there was no evidence supporting any impropriety. The employee did not use their NARA email account or any other agency resources in the conduct or promotion of their catering business, and the evidence showed that the employee only worked their catering business on weekends. The allegations were not substantiated.

Allegations of Directing Subordinates Not to Follow Regulations

The OI received an allegation that the subject had given a NARA employee an unlawful order to take an action violating Federal and NARA rules. Our investigation showed that the dispute rested on a communications failure. The subject's discussion with the employee had been overtaken by a subsequent ruling from OGC on the matter, which had not been communicated to the subject. The allegations were not substantiated.

Potential Hatch Act Violation

During the Hatch Act review of emails discussed above, one senior level employee was referred to the OSC.

Oversight

Assessment of NARA's Long-Distance Telework Policy

In March 2012, NARA instituted a telework policy (NARA Directive 332) establishing five telework classifications that would apply to eligible NARA employees. One classification, Long-Distance Telework (LDT), was designed for employees who telework at least eight days per pay-period. In this reporting period, the OI conducted a limited assessment of the implementation of the LDT classification and identified four programmatic deficiencies:

1. The Telework Coordinator, who serves as the point of contact for both NARA and for the Office of Personnel Management, does not receive copies of all LDT agreements. Centralization of LDT agreements with the Telework Coordinator is a requirement of the underlying Federal telework regulation.
2. Some LDT agreements are being approved only at the level of the employee's immediate supervisor, and are missing the "Executive/Director Level" approvals required by NARA Directive 332.
3. Time coding is not consistent among all employees who have LDT agreements.

4. Review, revision, and renewal of LDT agreements is not timely.

In its response, the agency stated that the noted deficiencies would be taken into consideration in the agency's ongoing improvement of the telework program.

Assessment of NARA's Holdings Steward Badge Policy

NARA permits specifically identified employees to remove holdings from NARA facilities for work purposes. The Security Management Division issues these employees a Holdings Steward Badge (badge), which is a photographic identification card with a fixed expiration date. In this reporting period, the Office of Investigations (OI) conducted a limited assessment of the Holdings Steward Badge program as it operated in two facilities in College Park, MD and Washington, DC. We identified four deficiencies:

1. Inconsistent policy/practices between the facilities with respect to (a) how date is recorded in the facilities' master badge rosters, (b) collecting expired badges, and (c) re-issuing badges with revised/renewed expiration dates.
2. There is no system alerting security officials to badges' imminent expiration, a system which would allow for the badges' timely collection and, if necessary, re-issuance with revised expiration dates.
3. Security officials do not always give presented badges close review. The OI conducted four test operations, two at each facility, during which security officials allowed simulated NARA holdings to be taken from the facility after a cursory badge review. Security failed to recognize badges that were either expired, or had been issued in a name and photograph different from the OI employee who presented the badge.
4. As currently interpreted and applied, an exit-review waiver for employee-identified lactation-related personal property does not properly fall under the Holdings Steward Badge program, and creates a "blind spot" or gap in holdings security.

The OI issued its assessment on December 15, 2016, and on February 3, 2017, the agency provided a comprehensive, point-by-point response addressing each of our findings and recommendations with revised and altogether new policies.

Employee Suspended for Refusing to Cooperate with Investigation

As part of an separate investigation, we identified one of the subject's co-workers as a potential witness to be interviewed. Initially, the witness refused to be interviewed without a union representative present; however, when a union representative arrived, the witness flatly refused to be interviewed under any circumstances whatsoever. The witness was informed that participation is compulsory and that further refusal could lead to punitive administrative action, but the witness again declined to cooperate. The witness was ordered by her supervisor to attend a second meeting, at which she was to be presented with a document clearly explaining her participatory obligations and the danger of punitive administrative action for noncompliance. However, the witness instead left the workplace and did not attend the meeting. The witness briefly attended a third meeting several days later, but gave only evasive and misleading responses before the attempt was terminated. The initial disciplinary proposal was for a seven-day suspension, but it was reduced to five days based on the deciding official's review of all mitigating and aggravating factors.

Relocation Incentive Repaid When Two-Year Employment Commitment Wasn't Met

In August 2015, a NARA employee accepted a lump-sum payment under $10,000 as incentive to relocate to a different state. As part of the Relocation Incentive Service Agreement that the employee signed, the employee committed to continue their NARA employment for at least two years. In September 2016, however, the employee accepted employment at another Federal agency. The employee was not required to repay the entire payment, but was assessed a pro-rated sum of less than half the amount. The employee acknowledged their debt, agreed to a monthly repayment plan, and has started making payments.

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. Hotline intakes which warrant further action may be processed as preliminary inquiries to determine whether they should be investigated as numbered investigations. Some Hotline intakes may not warrant further action by the OI. Where appropriate, referrals may be made to OIG audit staff, NARA management, or external authorities.

Hotline Activity for the Reporting Period	
Hotline and Complaints received	173
Hotline and Complaints referred to NARA or another entity	28

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 *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 NARA's FY 2016 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 FY 2016 Audit of NARA's Compliance with the Federal Managers' Financial Integrity Act for FY 2015 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 FY 2015 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 FY 2015 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 that while NARA appears to be aware of the significant risks and challenges it faces, the agency 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.

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. NARA's solution to address the system limitations is the ERA 2.0 Project. This is an on-going development effort with implementation currently planned for April/May 2018 and lifecycle costs estimated at $38 million. However, due to funding obstacles the project is experiencing delays.

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, on January 20, 2017, NARA received legal custody of over 270 terabytes of electronic records from the Obama administration. This is about three times more electronic records than what NARA received from the Bush administration. Searches of the Obama electronic records are currently being performed by a contractor to address special access requests while testing is conducted on the ERA Executive Office of the President's System prior to issuance of an authority to operate.

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 identified, scheduled, 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. Historically, the digitization approaches implemented by NARA were not large enough to make significant progress in meeting this goal. Further, due to poor planning and system limitations of the public-facing National Archives Catalog, 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.

Approximately 22 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 on which electronic records and audiovisual records are stored. 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 logical access control system compliant with Homeland Security Presidential Directive (HSPD-12). 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 with proper management support and visibility within the organization to adequately align acquisition functions with NARA's mission and needs. NARA is challenged with strengthening the acquisition workforce and to improve the management and oversight of Federal contractors. Lastly, NARA is challenged with strengthening internal controls over acquisition functions and providing better oversight and management of its procurement activities to ensure effective and efficient processes and procedures adhere to Federal and internal guidance.

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 for NARA to maintain security, data reliability, and accuracy as it strives to 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 agencies face conducting their activities and operations. The Circular provides updated implementation guidance to Federal managers to improve accountability and effectiveness of both Federal programs and agency mission support operations. According to the Circular, agencies should do this through implementation of Enterprise Risk Management (ERM) practices; and by establishing, maintaining, and assessing effective internal controls. 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 has yet to implement an 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. Additionally, without an effective ERM process in place that clearly identifies, categorizes, and assesses the effectiveness of controls related to key risks, the Archivist's annual assurance statement to the President and Congress may not clearly reflect NARA's current internal control environment, including risks.

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

IG Act § or Law	Subject	Page(s)
§ 4(a)(2)	Review of legislation and regulations	5 , 9
§ 5(a)(1)	Significant problems, abuses, and deficiencies discovered during the reporting period	2–5, 13–23, 24–29
§ 5(a)(2)	Significant recommendations for corrective action	2–4, 13–19
§ 5(a)(3)	Prior significant recommendations on which corrective action has not been completed	44–77
§ 5(a)(4)	Summary of prosecutorial referrals and convictions	26, 39
§ 5(a)(5)	Information or assistance refused and reported to agency head	42
§ 5(a)(6)	List of audit, inspection, and evaluation reports issued	40
§ 5(a)(7)	Summaries of significant reports	2–5, 13–23, 24–29
§ 5(a)(8)	Questioned costs in audits, inspections, and evaluations	40
§ 5(a)(9)	Funds put to better use in audits, inspections, and evaluations	41
§ 5(a)(10)	Prior audit, inspection, and evaluation reports with no management decision, no management comment, or unimplemented recommendations	42
§ 5(a)(11)	Significant revised management decisions	42
§ 5(a)(12)	Significant management decisions with which the OIG disagreed	31
§§ 5(a)(14), (15), (16)	Reporting on OIG peer review	10
§ 5(a)(17)	Statistical table on investigations and referrals	39
§ 5(a)(18)	Description of metrics used in § 5(a)(17) table	39
§ 5(a)(19)	Reporting on substantiated investigations of senior government employees	26–27
§ 5(a)(20)	Reporting on substantiated whistleblower retaliations	42
§ 5(a)(21)	Reporting on agency attempts to interfere with OIG independence	42
§ 5(a)(22)(A)	Closed inspections, evaluations, and audits not disclosed to the public	2–5, 13–23
§ 5(a)(22)(B)	Closed investigations of senior government employees not disclosed to the public	26–27
P.L. 110-181	Annex on completed contract audit reports	42
P.L. 104-106	Open audit recommendations	44–77

SUMMARY OF INVESTIGATIONS AND PROSECUTORIAL REFERRALS

Requirement 5(a)(4), (17), and (18)

Investigative Workload	
Hotline and complaints received and opened this reporting period	173
Hotlines and complaints referred to other parties during this reporting period	28
Investigations opened this reporting period	18
Investigations closed this reporting period	10
Investigative reports issued this reporting period	12
Investigative Results	
Total individuals referred to DOJ for prosecution	0
Individuals referred to DOJ – accepted for prosecution	0
Individuals referred to DOJ – declined for prosecution	0
Individuals referred DOJ – pending prosecution decision	0
Total individuals referred to state and local authorities for prosecution	1
Individuals referred to state and local authorities – accepted for prosecution	1
Individuals referred to state and local authorities – declined for prosecution	0
Individuals referred state and local authorities – pending prosecution decision	0
Arrest	1
Indictments and informations	0
Convictions	0
Fines, restitutions, judgments, and other civil and administrative recoveries	$0
Administrative Remedies	
Employee(s) terminated	0
Employee(s) resigned	1
Employee(s) suspended	3
Employee(s) given letter of reprimand or warnings/counseled	13
Employee(s) taking a reduction in grade in lieu of administrative action	0
Contractor (s) removed	0
Individual(s) barred from NARA facilities	0

The numbers in the table above were compiled by our electronic case management system, and only reference actions that happened within the reporting period. If the case was a joint case worked with another investigative office, the statistics above show the total numbers for the case and do not apportion numbers to each office. Investigative reports include only Reports of Investigation for numbered investigations.

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
17-AUD-01	Enterprise-wide Risk Assessment (performed by Cotton & Company)	10/28/2016	$0	$0	$0
17-AUD-02	Audit of NARA's Inventory System Tracking and Monitoring Process	11/4/2016	$0	$0	$0
17-AUD-03	NARA's Compliance with the Federal Managers Financial Integrity Act for FY15	11/4/2016	$0	$0	$0
17-AUD-04	Audit of NARA's Management Control Over MS Access Applications and Databases	11/18/2016	$0	$0	$0
17-AUD-05	Oversight of Consolidated Audit of NARA's Financial Statements	11/11/2016	$0	$0	$0
17-AUD-06	Audit of NARA's Procurement Program	11/15/2016	$0	$0	$0
17-AUD-07	Audit of NARA's Compliance with Homeland Security Presidential Directive 12	2/9/2017	$0	$0	$0
17-AUD-08	Audit of NARA's Adoption and Management of Cloud Computing Activities	3/15/2017	$0	$0	$0

AUDIT, INSPECTION, AND EVALUATION REPORTS WITH QUESTIONED COSTS

Requirement 5(a)(8)

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

AUDIT, INSPECTION, AND EVALUATION 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 (see note below)	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	$4,447
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	$9,069,395
E. For which no management decision was made within 6 months of issuance	3	$9,073,842

Note: OIG Advisory Report No. 12-08, NARA's Reliance on Legacy Systems to Meet Electronic Records Mission Needs, dated March 30, 2012 found that by not implementing many of the original requirements the ERA System lacks much of the functionality originally envisioned. This had resulted in NARA spending approximately $9 million to operate, maintain, and use eight older, outdated legacy systems that were supposed to be retired and/or subsumed with the implementation of the ERA system. While this does not flow directly from a numbered audit recommendation, we believe these issues are significant and should be publicly reported. The actual cost is likely much higher as these costs may be repeating annually. However, we do recognize NARA has been constrained in how they have been allowed to develop ERA. We hope to update this information soon as new audit work in this area is ongoing.

OTHER REQUIRED INFORMATION

REQUIREMENT	CATEGORY	SUMMARY
5(a)(5)	Information or assistance refused	None.
5(a)(10)	Prior audit reports with no management decision	Management has concurred or disagreed with all issued reports.
5(a)(11)	Significant revised management decisions	None.
5(a)(12)	Significant management decisions with which the OIG disagreed	See page 31.
5(a)(20)	Detailed description of instances of whistleblower retaliation, including consequences for the offender	No closed investigations this period substantiated whistleblower retaliation.
5(a)(21)(A)	Agency attempts to interfere with OIG independence with budget constraints designed to limit the OIG's capabilities	None.
5(a)(21)(B)	Agency attempts to interfere with OIG independence by resisting or objecting to oversight activities, or restricting or significantly delaying access to information	None rising to this level.

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 conducted audit work involving the ERA and other contracts during this period, they were generally program audits as opposed to contract audits.

Audit Recommendations Where NARA Has Assumed Risk

The following audit recommendations have been closed by the OIG 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. This list contains recommendations that NARA had assumed the risk for in prior periods.

Report Number	Title and Date	Rec. No.	Recommendation
08-01	08-01, Audit of NARA Artifacts *October 26, 2007*	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 *January 3, 2012*	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 *September 13, 2012*	1h	Appropriate storage hardware for the Reagan Library is procured and installed.
		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.
		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 *August 27, 2012*	12	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		13	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		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.
		44	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		45	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

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 46 audit recommendations were either closed or subsumed into other recommendations.

Report Number	Title and Date	Rec. No.	Recommendation
06-10	Evaluation of NARA's Affiliated Archives Program *August 9, 2006*	3	The Archivist should take appropriate measures to revise MOUs between NARA and affiliates to incorporate current standards for housing NARA records.
		4	The Archivist should ensure that there is a mechanism to update the MOUs. Specifically, a procedure should be established to update the MOUs on an interim basis, or when new standards are implemented at NARA.
		5	The Archivist should ensure that all MOUs contain the required clause for the use of the NARA seal.
		6	The Archivist should ensure that all affiliates meet the current storage standards or provide waivers and/or time frames to have the affiliates become compliant with the NARA 1571 standards.
06-11	Audit of System Adm. Rights and Controls *September 27, 2006*	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 *November 14, 2007*	13	The Assistant Archivist of Administration should direct the Director NAA to establish written policies and procedures to evaluate the effectiveness of cardholder reconciliations and approving officials' certifying duties.
08-05	FY 07 FISMA Review *March 20, 2008*	7	The Assistant Archivist for Information Services should add security vulnerabilities identified during the server audits to the system's plan of action and milestones to ensure proper tracking and visibility.
		8	The Assistant Archivist for Information Services should conduct "lessons learned" meetings in accordance with the guidance in NIST SP 800-61 when a major incident occurs and periodically for lesser incidents, and develop and implement a control mechanism to verify compliance.

[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.

		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.
08-07	Audit of the Researcher ID Card Program *April 24, 2008*	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 *September 29, 2009*	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 *April 2, 2010*	5	The Assistant Archivist for Records Services, Washington DC (NW) should ensure development of controls to adequately monitor agency scheduling of electronic records in an effort to reasonably ensure electronic records/systems are scheduled in timely manner, and therefore provide a reasonably accurate reflection of the universe of electronic records.
		6	The Assistant Archivist for Records Services, Washington DC (NW) should ensure a methodology for verifying the accuracy/completeness of Federal agency responses to electronic records scheduling requirements resulting from the E-Government Act of 2002.
		7	The Assistant Archivist for Records Services, Washington DC (NW) should ensure development and application of a methodology for adequately identifying gaps in electronic record accessions. This methodology should reasonably ensure permanent electronic records are identified, scheduled, and ultimately obtained by NARA.
10-07	Audit of NARA's Network Infrastructure *April 28, 2010*	10a	The CIO should implement multifactor authentication for network access to infrastructure devices.
		14	The Archivist should direct the Assistant Archivist for Information Services, Assistant Archivist for Regional Records Services, and the Assistant Archivist for Presidential Libraries to coordinate with the Assistant Archivist for Administration to develop a mechanism to track access reviews and key inventories for computer rooms and other locations where IT network infrastructure equipment is stored at the field sites.
10-14	Audit of the Process for Providing and Accounting for Information Provided to Researchers *August 6, 2010*	1	The Assistant Archivist for NW should establish formal written policies and procedures to improve NW monitoring of the pull and refile process.
		2	The Assistant Archivist for NW should implement a centralized database for all of the NW divisions involved in the processing of researchers' requests for records and determine the necessary information that should be included in the database.
11-02		1	NARA management apply the appropriate hot fix referenced in the vendor advisory on the affected machines.

	Network and Penetration Testing Oversight *November 8, 2010*	2a	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		2b	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		2c	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		3a	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		3b	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		3c	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		3d	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		6a	NARA management should immediately address corrective action for all vulnerabilities identified as "high" and "critical" risk.
		6b	NARA Management should evaluate the identified risks and corrective actions to address those identified as “medium" and "low" risk vulnerabilities.
11-05	Audit of Archives I & II Guard Service Contract *February 18, 2011*	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 *July 7, 2011*	2a	Develop and implement a mandatory specialized training course for travelers and authorizing officials reiterating their roles and responsibilities. Refresher courses should be provided on a periodic basis.
		2d	Develop and implement procedures to follow up on travel vouchers not submitted within five working days. Take appropriate action for people who do not comply within five working days.
11-15	Audit of NARA's Drug Testing Program *July 7, 2011*	2	Amend NARA TDPs to ensure compliance with the SAMHSA’s Interagency Coordinating Group Executive Committee Guidelines for the Selection of Testing Designated Positions and establish a mechanism to periodically review and update TDPs as necessary.
		3	Develop a training course for all supervisors that will aid them in recognizing and addressing illegal drug use by agency employees. This training should be mandatory for all supervisors. Also evaluate the current drug awareness training for employees.

		4	Develop a retention plan for all drug testing-related documentation consistent with the guidance issued by SAMHSA.
		5	Review NARA's Drug Free Workplace Plan and update it as necessary. In addition, a plan for periodic reviews and updates of the plan document should be developed.
11-20	Audit of NARA's Telework Program *September 30, 2011*	1d	Develop a method and common criteria for tracking telework participation.
		3a	The Executive for Information Systems, CIO, and Executive for Business Support Services should ensure all deferred and failed security tests have been reassessed and the results documented.
		3e	Review Citrix security configurations for adequacy.
12-05	Audit of the Management of Records at the Washington National Records Center *March 27, 2012*	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.
		8	The Executive for Agency Services should ensure management designs and implements monitoring activities for records processed at WNRC including weekly, monthly, and quarterly reports.
		12a	Procedures for all WNRC processes are documented. Review existing procedures and update as necessary.
		12b	Procedures between unclassified and classified processes are consistent where possible.
12-09	Audit of NARA's Data Center Consolidation Initiative *May 10, 2012*	1b	The CIO should update the Master System List and/or Enterprise Architecture to incorporate energy usage calculations.
		1c	The CIO should update the Master System List and/or the Enterprise Architecture to incorporate realistic estimates of funding needed or savings to be realized from implementing NARA's data center consolidation goals.
		1d	The CIO should update the Master System List and/or the Enterprise Architecture to incorporate annual savings metrics such as rack count reduction, server count reduction, energy usage reduction, and energy cost reduction to monitor progress.
		3	The CIO should conduct the consolidation/virtualization analysis to investigate the impact of consolidating or virtualizing two major application domains (NISP and ERA) and the General Support System (NARANET) as planned, or evaluate other alternatives to increase the average server utilization rate.
		4	The Executive for Business Support Services should evaluate the current organization of rack space and determine whether servers can be consolidated into fewer racks when considering space optimization, power consumption, operations management, and component failure/recovery perspectives.
12-10	Follow up Audit of Artifacts *September 13, 2012*	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.

		2b	Review and revise current time-guidance policy, as appropriate, for baseline inventories for newly established Presidential libraries.
		5b	Develop documentation guidelines that identify the importance of supporting the conclusion reported on the annual V/V reports. When counting objects, the support documentation should show the same count.
		7a	Policies and procedures are clarified and reiterated to library personnel concerning 1) sequestration of museum artifacts from library personnel other than museum personnel, and 2) procedures to periodically review access logs and security camera tapes.
		7b	Policies and procedures for artifacts on long-term loan are re-iterated and disseminated concerning 1) the annual update of loan agreements and 2) requirements for long-term loans including photo requirements. LP should establish time caps on loans or periodically request temporary return of items for condition assessments.
		7c	Reiterate NARA policy to adequately backup inventory-related collection documentation.
		8a	Update comprehensive set of museum collection management policies and procedures and ensure their development.
		8b	Establish procedures to periodically review and, if necessary, revise said policies and procedures.
12-11	NARA's Network Assessment Audit *August 27, 2012*	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.
		19	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		20	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		28	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		32	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		33	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		35	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		40	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.

		41	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		42	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		47	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		48	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
12-15	Audit of NARA's Classified Systems *July 23, 2012*	1	The Executive for Information Services/CIO (I), in coordination with the Chief Operating Officer (C), should ensure all classified system authorization packages are updated in accordance with NARA policy.
		2	I, in coordination with C, should establish a timeframe for review and approval of authorization documents.
		3	I, in coordination with C, should develop a continuous monitoring strategy for classified systems requiring system owners on at least a quarterly basis to assess security controls and inform authorizing officials when changes occur that may impact the security of the system.
		4	I, in coordination with C, should obtain authorizations to operate for each of the classified systems or disallow them in accordance with NARA and Federal policy.
13-01	Audit of NARA's Internal Controls Program for FY 2010 *December 10, 2012*	1d	Resources are employed to develop and implement the ICP including, but not limited to, a Chief Risk Officer, additional employees or contractors, and the purchase of appropriate ICP software.
		1e	Risk management responsibilities are included in the performance plans for program and function owners.
		1g	A Risk Management Policy is created to communicate NARA's commitment to enterprise risk management.
		1i	A training plan is developed that encompasses educating the agency on risks and internal control. Additional training is provided to all individuals responsible for executing the ICP, including program owners, function owners, and Management Controls Oversight Council (MCOC) members.
13-08	Audit of NARA's Preservation Program (Textual) *July 9, 2013*	1a	The Archivist should ensure an overarching preservation strategy is developed. Additionally, a risk-based approach to holistically assess the agency's preservation needs and design the agency's preservation plan should be implemented.

		1b	The Archivist should ensure an analysis is conducted of the organizational structure and responsibilities of each office involved in preservation. This should include a determination whether the preservation strategy can be effectively implemented with a decentralized structure, or if one NARA office should have authority over the entire Preservation Program.
		2	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services, should ensure comprehensive preservation policies and procedures for each of their organizations are developed and/or updated.
		3a	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services should completely identify the resources necessary to adequately accomplish NARA's preservation mission.
		3b	Develop a plan to identify the complete universe of textual and non-textual records that require preservation.
		4	The Executive for Research Services should ensure a detailed analysis is performed and communicate about the risks versus the benefits associated with not using the existing risk assessment data to calculate the backlog for the Washington area Archives.
		5a	The Executive for Research Services should ensure an analysis is performed to determine if additional risk assessments for the Washington area Archives and Presidential Libraries including older holdings should be completed. Identify the risks for not completing the assessments.
		5b	The Executive for Research Service should ensure additional measurable performance metrics are developed and implemented to track the progress within the Preservation Program.
		5c	The Executive for Research Services should ensure a cost benefit analysis for the HMS circulation Module is completed. Request required resources if the cost benefit analysis identifies benefits to the agency.
		5d	The Executive for Research Services should ensure Denver, St. Louis, and Special Media implement HMS to record risk assessments.
		6	The Executive for Legislative Archives, Presidential Libraries and Museum Services should ensure an analysis is performed to identify whether HMS should be implemented across the Libraries. If it is decided HMS will be implemented, a timeline should be established. If it is decided HMS will not be implemented, identify (1) how the existing system will meet the agency's preservation needs and (2) obstacles and risks for not implementing HMS.

13-09	NARA's Data Backup Operations *July 9, 2013*	4	The CIO should develop a process to regularly test data backups to verify information integrity.
		10	The CIO, the Director of Acquisition Services, and NARA's Office of General Counsel should review purchases made for offsite storage costs to determine whether NARA's procurement process and Federal appropriations laws were violated and if so take appropriate corrective action.
13-10	NARA Archival Facilities *July 19, 2013*	1a	The COO should ensure a comprehensive review of the Standards is completed. Additionally, roles and responsibilities for offices involved in the execution of the directive are clearly defined.
		1b	The COO should ensure a plan is developed including a timeline for when the archival storage facility reviews will be completed.
		1c	The COO should ensure an accurate listing of facilities currently compliant with the Standards along with the area of deficiencies is identified and communicated.
		1d	The COO should ensure resources needed to make all archival storage facilities compliant by 2016 are identified. If the facility cannot be brought into conformance with the Standards, determine and document what mitigating actions have been implemented.
		1e	The COO ensures Performance Measurement and Reporting System (PMRS) is updated to accurately reflect percentage of archival holdings in appropriate space.
13-11	Audit of ERA Ingest Efforts *September 19, 2013*	1	The COO assess Federal agency usage of Base ERA and implement a process to improve the records management workload and records management practices that exist between NARA and Federal agencies to ensure electronic records are being properly transferred into Base ERA.
		2	The COO identify the most efficient and effective method of ingest and require Federal agencies to follow this method when transferring electronic records into base ERA. In addition this information should be properly disseminated to Federal agencies.
13-12	Audit of the NARA IDS *September 10, 2013*	12	The CIO should ensure the preliminary reporting of all incidents and events reportable to US-CERT is made within the specified timeframes. Further details on the incident or event gathered after the original reporting should be communicated to US-Cert as an update.
		14	The CIO should ensure incident response tabletop exercises are conducted for staff performing and/or supporting computer security incidents on at least an annual basis, and practical and relevant topics to NARA's computing environment are covered within the exercises.
		15	The CIO should develop a policy for CIRT members to take training at least on an annual basis to ensure they remain up to date with current patterns/types of cyber attacks and effective, efficient incident remediation methodologies.

13-14	Audit of Processing of Textual Records *September 18, 2013*	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.
		2d	The Executive of Research Services should conduct a workload analysis to determine if resource allocation between AI and AII is appropriate.
		3a	The Executive for Legislative Archives, Presidential Libraries and Museums should analyze the backlogs at the pre-PRA libraries and create processing plans for reducing the backlogs at these libraries on a more accelerated basis.
		3b	The Executive for Legislative Archives, Presidential Libraries and Museums should (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.
		4	The Executive for Research Services and the Executive for Legislative Archives, Presidential Libraries and Museums, should work with the Performance and Accountability Office to reassess current processing goals and make changes to the goals.
		5a	The Executive for Legislative Archives, Presidential Libraries and Museums should work with the Performance and Accountability Office to develop a performance measure for tracking the process of electronic presidential records.
		5b	Determine the true backlog of electronic presidential records and determine if additional resources are needed and can be obtained to handle the increased workload.
		6	The Executive for Legislative Archives, Presidential Libraries and Museums and the Executive for Research Services should ensure a review is performed to validate the accuracy of processing data supplied to the Performance and Accountability Office.
		7	The Executive for Research Services should ensure procedures for all field locations are documented. Review existing procedures and update as necessary.
		8	The Executive for Legislative Archives, Presidential Libraries and Museums should ensure procedures for all Presidential libraries are documented, and review existing procedures and update them as necessary.
14-01	Oversight of NARA's Energy Savings Performance Contracts (ESPCs) *January 30, 2014*	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 *March 5, 2014*	4	Presidential libraries should work with NARA's general counsel to institute general counsel review program of a sample of applications for use (16011 forms) from all Presidential libraries to ensure the forms meet the requirements of 36 CFR 1280.94.
		5	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 *March 11, 2014*	2	NARA should ensure all field office contracting officers and buyers are adequately trained on how and when to close out NARA contracts. Additionally, periodic monitoring and testing of closeout procedures should be conducted to ensure contracts are closed out in a timely manner.
		3	NARA should establish and implement a formal documented process for informing the field office support team of field office contracts requiring review prior to award.
		4	Update NARA policies to ensure the guidance for approval of small and small disadvantaged business utilization exceptions is consistent.
14-08	Audit of NARA's Capital Planning and Investment Control (CPIC) Process *April 17, 2014*	1b	The CIO should ensure all required CPIC related documentation is completed for all NARA IT investments going through the CPIC process.
		1c	The CIO should require the creation and use of a checklist outlining the IT governance related documentation required to be completed for all IT investments going through the CPIC process.
		2	The CIO should require NARA's updated CPIC policies and procedures meet the CPIC process requirements detailed in the Clinger Cohen Act.
		3	The Chief Operating Officer (COO) should ensure NARA IT investments do not bypass NARA's CPIC process.
		5	The COO should ensure I-P maintains documentation of its approval of IT investments in PRISM and I-P's PRISM approval of IT investments is tested on an annual basis with all documentation of this testing sent to NARA's internal controls group.
		6	The COO should ensure the training guide for purchase card holders is updated to include a discussion of the requirements of NARA's CPIC Process.
		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.
14-09	Audit of Conference-Related Activities and Expenses	2a	The Chief Financial Officer (CFO) should ensure communication is provided to offices regarding adherence to conference policies, including penalties for non-compliance.

	May 1, 2014	2b	The CFO should ensure interim guidance 165-1, Conference-Related Activities and Expenses, is updated to incorporate statutory requirements for reporting to the OIG any conferences where expenses exceed $20,000.
		2c	The CFO should ensure methodology is developed for gathering and reporting post-conference details, including details of all expenses and justification when total costs increase by a threshold established by management. This should include a time frame for reporting.
14-10	Audit of NARA's Enterprise Wireless Access *May 9, 2014*	1d	NARA should assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements.
		1e	NARA should authorize network operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable.
		1f	NARA should monitor the security controls in the network on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analysis of the associated changes, and reporting the security state of the system to designated officials.
		3	NARA should develop, document, review, update, and implement wireless policies and procedures on at least an annual basis in accordance with internal NARA and NIST requirements.
		4a	NARA should utilize existing WLC and WAP baseline configurations or develop its own baseline configurations.
		4b	NARA should implement a process to monitor the WLC and WAP settings for compliance with the established baseline configurations.
		4c	NARA should document and approve any deviations from the WLC and WAP baseline configurations.
		4d	NARA should maintain older versions of the baseline configurations as necessary.
		5a	NARA should implement a process to conduct vulnerability scans that identify weaknesses related to NARA's wireless environment.
		5b	NARA should develop procedures to analyze and remediate the vulnerabilities identified.
14-11	Audit of Special Telework *May 5, 2014*	1	The Chief Human Capital Officer (CHCO) should develop controls and relevant control activities to ensure telework agreements are in place, reviewed, and renewed by the employee and the supervisor annually, and a copy of the approved, disapproved, or terminated telework agreement is provided to the NARA Telework Managing Officer.
		2	The CHCO should provide clarifying guidance to supervisors as to which arrangements require executive or staff director approval.

		3	The CHCO should establish an oversight mechanism to ensure employees' duty station assignments are reviewed and validated periodically.
		5	The CHCO should issue additional guidance for long-distance telework arrangements to require supervisors to conduct a cost/benefit analysis of the proposed arrangement and document this analysis. For those arrangements resulting in additional costs to NARA, supervisors should be required to justify how the arrangement is in the best interest of NARA.
		8	The CHCO should revise the Telework Agreement (form 3040) or issue additional guidance for full-time and long-distance telework to require supervisors and employees to estimate the timeframe for the arrangement, while still subject to the annual renewal.
		9	The CHCO should revise NARA 332 to include a requirement that new telework agreements be prepared and signed when a new employee/supervisory relationship is established.
		11	The CHCO should communicate best practices for monitoring telework employees and best practices in establishing special telework arrangements across the agency.
14-12	Audit of Selected Aspects of NARA's Digitization Program *July 3, 2014*	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 *October 24, 2014*	1	Develop new policies and procedures or update existing policies and procedures for at least the 11 programs areas included in the annual FISMA review.
		2	Coordinate with the Office of Performance and Accountability and 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 *November 12, 2014*	1a	Develop and document a strong internal control process for ordering, activating, and deactivating mobile devices and phone lines to ensure no unnecessary phone lines exist and incur costs.
		1b	Develop and document a strong internal control process for reviewing monthly bills for items including user names, activities, plan adequacy, and opportunity for cost savings.
		1c	Develop and document a strong internal control process for determining when an additional charge will be considered for reimbursement.
		2	Review and update NARA's current policy documents for use of NARA-issued mobile devices, including NARA 813-1 and NARA 802 to reflect more complete and accurate information an acceptable uses of the devices and when a disciplinary action will be requested.

		3	Provide training to educate users on acceptable uses of NARA-issued mobile devices, including requesting a travel device for international travel.
		4	Develop a formal policy for interaction of NARA-issued mobile devices with other systems and update NARA 813-1 to clearly reflect the policy.
		7a	Develop a comprehensive lost mobile device control process to include all lost or stolen mobile devices are managed on a centralized list with detailed information such as user's name, phone number, date lost/stolen and found, and status.
		7b	Develop a comprehensive lost/stolen mobile device control process to include the Remedy incident management system and ensure any task requiring contractor effort is appropriately communicated to ensure that data on all list of stolen devices is safeguarded.
		8a	Develop and document policies and procedures on maintaining a complete and accurate inventory providing traceability of the user, phone number, physical location, and the dates the device was returned, disconnected, and wiped.
		8b	Develop and document policies and procedures on mobile device retirement management process, defining the steps needed to be performed, by responsible party for each step, and the monitoring and reporting process.
15-03	Audit of Specially Protected Holdings *February 6, 2015*	1	Ensure NARA 1572 is updated to require custodial units to report their storage methods and exact containers locations and names of staff members and the specific areas to which they have access to BX.
		2a	Security Management performs initial certifications of Specially Protected Holdings (SPHs) storage areas.
		2b	Security Management performs security inspections of SPHs storage areas.
		2c	Security Management develops guidelines for SPHs security inspections, including timeframes, criteria, documenting requirements, and reporting requirements.
		3	Ensure an analysis is performed to determine if staff with access to SPHs, positions should be designated higher than low risk positions. Based on the analysis, nominate selected staff for required background investigations.
		4	Ensure Security Management maintains copies or obtains access to SPHs inventory listings and use them to randomly select records and verify their condition and location during inspections.
		5a	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.

		5b	Ensure inventory listings are reviewed to determine their accuracy and update as necessary.
		5c	Ensure a finding aid is created for the agency's entire SPHs collection at the item level.
		5d	Ensure locked hard copies of the inventory listings are maintained.
		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.
		6	Ensure NARA 1572 is updated to include (1) responsibilities for Security Management to review annual inspections, including documenting the review, for compliance with NARA 1572, (2) timeframes for when Presidential Libraries and Field Office Archives should complete annual inspections, and (3) the amended requirement for annual inspection reports to include the date of the inspection, individuals that complete the inspections, and a listing of items inspected, including their location and physical condition.
		7	Ensure all Presidential Libraries are in compliance with NARA 1572 policy of conducting annual inspections.
		8a	Initial inspections of SPHs inventory are completed.
		8b	Custodial units are in compliance with NARA 1572, including randomly inspecting at least 3% of SPHs inventory annually on a rotating basis and using one individual that does not work for the individual responsible for the inspection.
		8c	Annual inspection reports include at a minimum date of inspection, individuals that complete the inspections, and a listing of items inspected, including their location and physical condition.
		8d	Annual inspection results are adequately documented and communicated to Security Management and office heads.
		9a	Staff is properly trained or retrained to use charge out cards whenever records are removed from SPHs storage areas.
		9b	Access to SPHs storage areas is properly monitored, including keeping the list for who has access to the SPHs areas updated at all times and restricting access to only authorized staff.
		10a	Required elements for the handling of SPHs for each record storage area should be communicated to each custodial unit.
		10b	Detailed procedures are documented for each custodial unit.
		10c	A process is in place for periodic review of procedures and updates are made as needed.
15-10	Audit of Digitization Partnership Process	1	Conduct an agency-wide inventory of Digitization Partnerships and update NARA's partnership webpage to reflect current partners.

	March 30, 2015	2	Establish criteria for which Digitization Partnerships require public notification and approval by the Archivist of the United States.
		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 *May 5, 2015*	4	Develop agency-wide policies and procedures for digital file preservation.
		6	Develop a long-term strategy for increasing transfer capabilities between various internal storage systems housing digitized records.
		8	Work with partners to return partner-provided hard drives.
15-13	Audit of HR Systems and Data Accuracy *August 24, 2015*	1	Fully implement the new supervisor information update process in FPPS and conduct a review of the information on a periodic basis to ensure the information remains accurate and complete.
		4a	Create an Employee Locator update policy including the following: a defined timeframe within which employees are required to review and update Employee Locator entries.
		4b	Create an Employee Locator update policy including the following: supervisors' responsibility to ensure employee contact information remains complete and accurate
		5	Include in the new hire orientation the requirement to update Employee Locator entries, based on the policy created from recommendation three.
		10	Re-evaluate the option to utilize eCStaffing to manage personnel data for non-Federal workforce at NARA and use the HRMS as the single authoritative data source for the HSPD-12 LACS implementation.
		11	Establish on authoritative data source that provides the latest data to role-based users on NARA's Federal employees, contractors, and volunteers at the enterprise level.
15-14	Audit of Space Management for Paper Records *September 29, 2015*	1	Consider implementing records management guidance to make agencies report to NARA records in their possession 30 years or older on a more regular basis.
		2	Implement a strategy to work with other Federal agencies to resolve "limbo" records and schedule those records for accessioning or disposal.
		3	Work with R to facilitate consistent application of HMS at all archival facilities, to capture all archival holdings in HMS, and improve how HMS calculates the available space.
		4	Establish a permanent group to both track and manage space and advise NARA management on space matters across the agency.
		5	Develop a long-term space management strategy for the agency.
		6	Develop cost estimates for potential solutions.

		7	Incorporate space management into NARA's strategic planning initiatives and include the agency's space need in all necessary reporting. Considering reporting space management as a Material Weaknesses and track it appropriately
		8	Create a timeline for the agency to have necessary discussions with both internal and external stakeholders to address NARA's space challenges.
		9	Develop requirements necessary for NARA to prepare a budget request to address the agency's critical space challenges. After a strategy is implemented and requirements are developed, prepare and submit a budget request.
15-15	Cabling Audit *September 30, 2015*	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.
		2.1	Ensure that neat cable management and labeling mechanisms are employed for all sites.
		2.2	Ensure that all server rooms are equipped with appropriate fire detection and suppression capabilities.
		2.3	Limit access to all server rooms to those individuals with an explicit need to access IT equipment.
		2.4	Ensure that appropriate temperature and humidity monitoring and control mechanisms are employed for all server rooms.
		2.5	Ensure that appropriate UPS devices are employed for hardware supporting the site's network infrastructure.
		2.6	Ensure that all server racks, switches, and network equipment are adequately secured from unauthorized access via locked racks.
		3	NARA 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 *October 19, 2015*	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
		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
		3	The CIO and CINO should clearly define the roles and responsibilities throughout the process developed in recommendation #2
		4	The COO should coordinate with the CINO to develop a comprehensive list of public facing websites.
		5	The CIO and NGC should review and document the approval of all agreements for web hosting services.

		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.
		7	The CIO should coordinate with the CINO to make the web hosting environment FISMA compliant.
		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.
		9	The CIO should develop and document a process by which Information Services regularly communicate (no less than monthly) with Innovation.
		10	The CIO should provide Innovation with guidance that clearly delineates the management responsibilities of the web hosting environment between Information Services and Innovation.
		11	The CIO should provide training to Innovation regarding its responsibility as a System Owner.
		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.
		13	The CIO should require an IT security assessment be performed prior to NARA initiating a web hosting agreement.
		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.
		15	The CIO should ensure Information Services personnel document their review of the IT security assessments.
		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.
		17	Develop a process for managing access to shared user accounts.
		18	Implement the annual compliance check required by the User Account Management Standard Operating Procedure for Administrator accounts to the shared user accounts.
		19	Coordinate with Information Services to develop and document a plan to recover the other NARA-hosted websites besides Archives.gov.
		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.

		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.
		22	The CIO should encrypt NARANet backup tapes.
		23	Develop a current baseline configuration for the Solaris web servers.
		24	Apply the baseline configuration to the web servers.
		25	Coordinate with Innovation to configure the WebStage server to mirror the production web servers.
		26	The CIO should require all systems develop a baseline configuration document and have it approved before it is applied to the entire system.
		27	The CIO should develop controls to ensure all deliverables are provided before a RFC/RFW ticket for the web hosting environment is closed.
		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.
		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.
		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.
		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.
		32	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
		33	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.
16-02	Audit of NARA's Compliance with FISMA, As Amended *January 16, 2016*	1	For systems utilized by NARA and managed by Cloud Service Providers, NARA should develop and implement formalized procedures to ensure controls for which NARA has a shared responsibility are reviewed on an annual basis, documented and assessed as to the impact to NARA of any risks that may be present.
		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.

		3	NARA should configure RRS application password settings in accordance with NARA policy
		4	NARA should develop, update and implement formalized access control policies and procedures for the B&A, RRS, SCTS and DCU systems.
		5	NARA should implement and document user access reviews for B&A, ENOS/HMS, RRS, SCTS, and DCU.
		6	NARA should develop and implement procedures to reissue shared/group account credentials when individuals are removed from B&A and RRS user groups.
		8	NARA should develop, update and implement formalized VPN access policies and procedures to ensure individuals are granted appropriated access.
		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
		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.
		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.
		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.
		14	NARA should add an addendum to current agreements which requires compliance with NARA's information security requirements.
		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	NARA should develop contingency plans and disaster recovery plans for SCTS and B&A, and any other systems identified as critical.
		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.
		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.
		19	NARA should establish and document a detailed process to perform a comprehensive annual information system component inventory count.
		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 · 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 *March 4, 2016*	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.
		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.
		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 eliminate any accounts no longer needed.
		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.

		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.
		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.
		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.
		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.
		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.
		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.
		4	Ensure control procedures under NARA Directive 1608, Protection of Personally Identifiable Information (PII), are followed.
		6	Ensure all Federal Records Centers are following key control procedures under NARA Directive 271, Key Control at NARA Facilities.
		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.
		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.

		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.
		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.
16-05	Audit of NARA's Publicly-Accessible Websites *March 25, 2016*	1a	The CINO should 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.
		1b	The CINO should 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.
		1c	The CINO should 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.
		1d	The CINO should 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.
		1e	The CINO should 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.
		1f	The CINO should 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.

		1g	The CINO should 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.
		1h	The CINO should 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.
		1i	The CINO should 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.
		1j	The CINO should 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.
		1k	The CINO should 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.
		3	The CIO should implement secure HTTPS configurations for all publicly-accessible websites.
		4	The CIO should regularly scan (at least quarterly) all publicly-accessible websites to determine if HTTPS is securely configured.
		5	The CIO should document a process to review all security assessments by a qualified official.
		6	The CIO should ensure Information Services personnel review all cloud hosting security assessments.
		7	The CIO should ensure Information Services personnel document their review of the IT security assessments.
		1l	The CINO should 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.

16-07	NARA's Refile Processes at Selected Federal Records Centers *May 17, 2016*	1	The Executive for Agency Services should develop a plan to eliminate the backlog at each FRC.
		2	The Executive for Agency Services should 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.
		3	The Executive for Agency Services should 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.
		4	The Executive for Agency Services should coordinate with the IRS to receive more detailed information, including record listings, to allow for improved tracking of IRS records at FRCs.
		5	The Executive for Agency Services should establish standardized procedures for verifying batch volumes.
		6	The Executive for Agency Services should coordinate with the Director of the specific FRC to make all necessary reports concerning the missing record.
		7	The Executive for Agency Services should update the batch signoff process requiring employees to attest every item included in a batch was properly refiled or interfiled.
		8	The Executive for Agency Services should implement consistent unique batch numbering processes at the FRCs.
		9	The Executive for Agency Services should implement standard IRS document locators at the FRCs.
		10a	The Executive for Agency Services should 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.
		10b	The Executive for Agency Services should 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.
		10c	The Executive for Agency Services should establish standardized policies and procedures for the quality control reviews at the FRCs, including establishing timeframes for when the reviews must be conducted.

		10d	The Executive for Agency Services should 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.
		10e	The Executive for Agency Services should establish standardized policies and procedures for the quality control reviews at the FRCs, including determining the appropriate method for reviewing interfiles.
		10f	The Executive for Agency Services should 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.
		10g	The Executive for Agency Services should 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.
		11	The Executive for Agency Services should conduct training for all employees on the policies and procedures for quality control reviews, including notification of errors and penalties.
		12	The Executive for Agency Services should 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.
		13	The Executive for Agency Services should implement a mechanism (database, etc.) to facilitate the problem tracking and resolution process.
		14	The Executive for Agency Services should identify a resolution for the fifty-six boxes of IRS records maintained in the IRS refile room
17-AUD-01	Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls *October 28, 2016*	1a	The Chief Operating Officer/Chief Risk Officer should fully implement all components of NARA 160, including developing, documenting, and fully implementing NARA 162, *NARA's Enterprise Risk Management Program*. Within NARA 162, roles and responsibilities for ERM activities should be clearly identified.
		1b	The Chief Operating Officer/Chief Risk Officer should fully implement all components of NARA 160, including developing, documenting, and fully implementing NARA 163, *NARA's Issues Management*.
		2a	The Chief Operating Officer/Chief Risk Officer should develop, document, and implement a formal process to identify and prioritize risks within the organization. Risks should be tied directly to NARA's strategic plan and mission and prioritized based on their overall importance to the agency.

		2b	The Chief Operating Officer/Chief Risk Officer should develop, document, and implement a formal process to prioritize risk management activities, including the use of limited resources based on key risks within the organization. Management's prioritization should be clearly documented and include formal steps to ensure risks are maintained at an appropriate level.
		3	The Chief Operating Officer/Chief Risk Officer should provide additional resources to the Office of Accountability to ensure ICP activities are effectively carried out.
		4a	The Chief Operating Officer/Chief Risk Officer should develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review to ensure all required documentation has been submitted by the due date. Where documentation has not been provided, NARA should have a formal process in place to follow up and obtain the required documentation.
		4b	The Chief Operating Officer/Chief Risk Officer should develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review of ICP documentation submitted to ensure it is both complete and accurate. Where discrepancies are identified, NARA should have a formal process in place to follow up with management so corrections can be made.
		4c	The Chief Operating Officer/Chief Risk Officer should develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review of each office's submission to determine whether risks identified and conclusions made are appropriately supported.
		4d	The Chief Operating Officer/Chief Risk Officer should develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review of test plans and test results for all high-risk or highly critical functions to ensure they clearly demonstrate the office's methodology for performing testing and reaching conclusions.
		4e	The Chief Operating Officer/Chief Risk Officer should develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review of monitoring plans and monitoring results for all functions that clearly show the extent of monitoring performed, the office's methodology for performing the monitoring, and the rationale for its conclusions.

		5	The Chief Operating Officer/Chief Risk Officer should develop and fully implement a formal ICP training program. NARA's ICP training program should identify and require individuals who are involved with NARA's ICP to complete initial training and refresher training periodically thereafter. Further, management should track completion of ICP training to ensure all individuals involved in the ICP process have received adequate training.
		6	The NARA General Counsel should develop, document, and fully implement policies and procedures to ensure NARA personnel (i.e., employees, contractors, and others with access to NARA systems or information) review and formally acknowledge their responsibilities to comply with NARA's privacy rules of behavior annually.
		7	The NARA General Counsel should implement a process for following up on outstanding system change inquiries and obtaining the requested information.
		8	The NARA General Counsel should develop, document, and implement policies and procedures to periodically test the effectiveness of privacy policies, procedures, and controls.
17-AUD-02	Audit of NARA's System Inventory *November 4, 2016*	1	The CIO should develop, document, approve and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c).
		2	The CIO should ensure all of the systems managed by NARA and its contractors are included in the inventory.
		3	The CIO should update the inventory annually to ensure the information populated in the inventory is complete and accurate.
		4	The CIO should document in NARA Directive 101 the organization responsible for maintaining the system inventory.
		5	The CIO should comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are categorized.
		6	The CIO should comply with FIPS 199 and NIST SP 800-60 to ensure the categorization of information systems is accurate.
		7	The CIO should update the FIPS 199 guidance to include all information types listed in NIST SP 800-60 Volume II.
		8	The CIO should coordinate with system owners on validating their current FIPS 199 to ensure the systems categorization level is accurate.
17-AUD-03	Audit of NARA's Compliance with the Federal Managers Financial Integrity Act for FY15 *November 4, 2016*	1	The Archivist should provide the staffing resources necessary to provide sufficient coverage of the risks and internal controls of the agency.
		2	The Archivist should implement or upgrade current internal control software or utilize other mechanisms to enhance and improve the agency's ability to track and report on internal controls.
		3	The Archivist should ensure formalized internal control training is provided to NARA staff.

		4	The Archivist should ensure the MCOC tracks and manages all high-level risks.
		5a	The Archivist should address outstanding recommendations from OIG Audit Report No. 13-01, including ensuring development and implementation of NARA's ERM policy.
		5b	The Archivist should address outstanding recommendations from OIG Audit Report No. 13-01, including revisiting his decision on the placement and role in the organization of the Chief Risk Officer.
		6a	NARA Executives should ensure monitoring and testing plans are sufficiently reported in the ICP Tool.
		6b	NARA Executives should ensure results of monitoring and testing plans are achievable within the reporting timeframe.
		6c	NARA Executives ensure all information is up-to-date and reflects the current control environment.
		7	NARA Executives should identify, develop, and include in ICP reports measurable indicators to evaluate functions.
		8	NARA Executives should update NARA Directive 101 to include internal control responsibilities for each office.
		9	The ICP Official develop and implement a consistent risk assessment process and format for risk ranking, analysis of effect or impact, and risk reporting.
		10	The ICP Official should review the ICP reports and make and document any revisions necessary to the format to ensure all necessary information is obtained in the reports.
17-AUD-04	Audit of NARA's Management Control Over Microsoft Access Applications and Databases *November 18, 2016*	1	The CIO should, in conjunction with each program office, evaluate the Microsoft (MS) Access applications/databases used in each program office to determine if they are critical to the mission of NARA and/or each program office.
		2	The CIO should, in conjunction with each program office, implement the security assessment process as described in NARA's Enterprise Architecture to those applications/databases determined critical to carrying out NARA's or program offices' missions from Recommendation 1.
		3	The CIO should, in conjunction with each program office, develop and implement a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system.

		4	The CIO should, in conjunction with each program office, determine all MS Access databases containing PII and ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.
		5	The CIO should, in conjunction with each program office, develop and implement a process, for future MS Access applications and databases created by program offices, including notification to and approval from the Office of Information Services for those that are mission-critical and/or contain PII or otherwise sensitive information.
		6	The CIO should, in conjunction with each program office, identify all MS Access applications/databases containing programming languages and/or are source data for PMRS.
		7	The CIO should, in conjunction with each program office, ensure availability of rollback versions of applications/databases in the event they don't properly convert to MS Access 2013.
		8	The Chief of Management and Administration consider standardizing PMRS's source-pull method in order to minimize potential for human error when developing PMRS 2.0.
		9	The Chief Operating Officer, in collaboration with the OIG, issue an annual reminder to NARA staff of their responsibilities to cooperate with OIG audit requests, in accordance with NARA Directive 1201, the IG Act, as amended, and Title 18 U.S.C., Chapter 73, Section 1516, *Obstruction of Federal Audit*.
17-AUD-05	Audit of National Archives and Records Administration's Fiscal Year 2016 Consolidated Financial Statements *November 11, 2016*	1	The CIO should develop and execute a realistic holistic IT plan with target dates to resolve longstanding issues over access controls, security management, segregation of duties, and configuration management.
		2a	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing improved processes to ensure the timely removal of system access for separated employees and strengthen Supervisor training related to the employment separation process.
		2b	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing improved processes for the periodic review of network and financial applications to identify and remove inactive accounts on systems and networks. Recertify that access remains appropriate and is restricted to necessary personnel.

		2c	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing enhanced processes to secure physical access controls to sensitive areas.
		2d	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing a process for monitoring network audit logs for unauthorized or unusual activities. Implement procedures for analyzing network audit logs and ensuring such logs are maintained in accordance with NARA policy.
		2e	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing processes to ensure that default and easy to guess passwords are changed and all passwords are transmitted securely and encrypted.
		2f	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing improved processes for reviewing and updating key security documentation, including system security plans on an annual basis. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable federal standards.
		2g	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing improved processes for user account management to ensure assigned user permissions are commensurate with assigned position responsibilities.
		2h	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including strengthening patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure.
		2i	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including fully completing the migration of applications to vendor supported operating systems.
		2j	The CIO should continue to analyze and prioritize remediation efforts to accomplish security and control objectives, including implementing improved change control procedures to ensure the consistent testing of system changes for NARA financial applications.

17-AUD-06	Audit of NARA's Procurement Program *November 15, 2016*	3	The Chief Acquisition Officer (CAO) should formally appoint a Senior Procurement Executive (SPE) and procurement officials who are authorized to approve warrants over $100,000,000 and approve warrant for construction and architectural-engineering services contracting officers.
		4	Competition Advocate, in collaborations with the CAO, should complete an evaluation and report on the overall strength of NARA's competition practice in accordance with the Federal Acquisition Regulations (FAR) and OMB guidance.
		5	Competition Advocate, in collaborations with the CAO, should develop and implement procedures to promote the acquisition of commercial items and report annually new initiatives to the CAO and SPE.
		6	The CAO should develop and implement procedures to ensure contracting offices in Acquisitions Branch (BCN) and Space Planning and Projects Branch (BFS) report all contract related activity to the SPE.
		7	The CAO should ensure NARA 501 NARA Procurement policy and NARA's General Acquisition Policy addresses procurements related to Architecture/Engineering and Construction.
		8	The CAO should, in collaboration with CFO, Director of Acquisitions, and program managers, develop and implement procedures for proper planning of new contracts with NARA funds.
		9	The CAO should develop and implement procedures to ensure contracts are evaluated to identify contracts that are wasteful, inefficient, or unlikely to meet NARA needs.
		10	The CAO and SPE should develop and implement test plans and procedures to assess internal control over acquisition activities and programs using OMB Memorandum, *Conducting Acquisition Assessments*.
		11	The CAO should modify procedures to ensure all contracting activity, including Architecture/ Engineering, construction services are included in random selections for internal control reviews.
		12	The CAO should establish standards for retaining documentation supporting the evaluation of internal controls.
		13	The CAO should include Contracting Officers who are not GS1102's, Contracting Officer Representatives and Program and Project Managers in the internal control program test plan.
		14	The CAO should establish various performance metrics to be tracked and analyzed on how long the acquisition takes, where delays occur and why delays occur.
		15	The CAO should develop and implement meaningful and measurable performance metrics to continually assess the performance of the acquisition function in supporting NARA's mission and achieving acquisition goals.

		16	The CAO should ensure NARA 501 NARA Procurement policy include guidance to program offices on their responsibilities in the procurement process.
		17	The CAO should ensure program offices are routinely trained in NARA procurement policy and procedures, specifically procurements requisition packages and procurement lead times.
		18	The CAO should assess staffing needs for NARA's Procurement Program to ensure the procurement program has sufficient staff to maintain effective, efficient operations and adhere to Federal and internal guidance.
		19	The CAO should develop a process to monitor the close-out of contracts process to ensure contracts are closed in a timely manner and identify reasons contracts are not closed out in a timely manner.
		20	The Acquisition Career Manager (ACM) should verify all contracting officers, contracting officer representatives, program and project managers, and other contracting professionals set up an account in Federal Acquisition Institute Training Application System for tracking certifications and continuous training.
		22	The CAO should work with the CIO to determine and document how best to support IT acquisition, such as through the development of specialized IT acquisition cadres, specifically contracting officers, and staff.
		23	The ACM should ensure NARA Certification for Program and Project Managers Applications are signed by the Deputy Archivist in accordance with NARA policy and maintained.
		24	The CAO should ensure all contracting officers, regardless of their government series, be certified at an appropriate level; and any contracting professional issued an unlimited warrant be level III certified.
		25	The CAO should establish and implement procedures for potential administrative or disciplinary actions for contracting officers, and contracting officer representatives, and other contracting professionals that do not have their Federal Acquisition Certifications or continuous trainings required by OMB guidance. For example, if after one year from notice the contracting professional still does not have appropriate certificates and/or training, disciplinary action, removal of warrant or removal from the position may occur.
		26	The CAO should ensure there is more IT training for CO's that do a significant amount of work in IT in accordance with OMB technology acquisition cadre guidance.

17-AUD-07	Audit of NARA's Compliance with Homeland Security Presidential Directive 12 *February 9, 2017*	2	Chief of Management and Administration or designee should develop a detailed implementation plan with remaining work to be completed, critical tasks, roles and responsibilities of key personnel, milestones for critical tasks, costs, locations, and any other necessary documentation that would allow the agency to successfully implement Homeland Security Presidential Directive 12 (HSPD-12).
		3	Chief of Management and Administration or designee should use existing budgetary resources to fully implement HSPD-12.
		4	Chief of Chief of Management and Administration or designee should establish a reasonable date to fully implement HSPD-12.
17-AUD-08	Audit of NARA's Adoption and Management of Cloud Computing *March 15, 2017*	1	The CIO should, acting as the centralized authority for NARA's cloud computing program, should take the lead and collaborate with business areas such as Acquisitions and General Counsel, to develop, approve, and implement comprehensive policies and procedures which will coordinate activities and establish key control points for NARA's cloud computing program.
		2	The CIO should complete and document a review of existing IT systems for cloud compatibility.
		3	The CIO should update the Enterprise Cloud Strategy with clearly defined roles and responsibilities, and develop and implement a written plan to execute the strategy.
		4	The CIO should conduct and document a risk assessment specific to NARA's implementation of cloud computing in coordination with NARA's Chief Risk Officer.
		5	The CIO should develop, approve, and implement written NARA-wide standards for the early identification and designation of cloud computing services, and consistently communicate the standard to those who need it.
		6	The CIO should establish and approve a centralized reporting point for cloud computing inventory and develop, implement and communicate a written mechanism to standardize tracking cloud computing inventory across NARA's business area lines.
		7	The CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop, approve, and implement its written cloud provisioning guidelines.
		8	The CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop, approve, and implement its IT Security Contractual Requirements in addition to a method to monitor and enforce the use of the standards.

		9	The CIO, in conjunction with Acquisitions and General Counsel should develop, approve, and implement written standards for centralized maintenance and standardized monitoring of service level agreements and formally communicate the requirement to those who need it.
		10	The CIO should coordinate with the Chief Acquisitions Officer, and General Counsel to establish a working group to evaluate and monitor recommendations and best practices for cloud computing procurement in order to improve the content and effectiveness of the CPIC Business Case Form.