NATIONAL ARCHIVES

OFFICE *of* INSPECTOR GENERAL
NATIONAL ARCHIVES

OFFICE *of* INSPECTOR GENERAL

SEMIANNUAL REPORT *to* CONGRESS

OCTOBER 1, 2019 *to* MARCH 31, 2020

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, 2019 to March 31, 2020. While the onslaught of COVID-19 has affected the world in profound ways changing how we interact and work, the OIG continues our work, and we are determined to persevere.

At the end of this reporting period the OIG had implemented a special policy to handle COVID-19, closed our physical office for safety, and was teleworking full time. Even as this virus altered our fundamental understandings of how to act as a society, the OIG staff stood strong and continued to carry out our mission. Our audits proceeded, investigations continued, and the work of the OIG carried on in new ways. I see how the OIG staff has adapted and succeeded in the face of this shared adversity, and I am in awe. I am truly thankful for the Herculean efforts I know the staff are putting in to educate their children, keep their loved ones as safe as possible, and adapt to new ways of living; all the while continuing to drive the OIG and NARA forward. This has been no small task and will undoubtedly continue for quite some time. These efforts do not go unnoticed, and I am grateful.

Accordingly, the products described in this report demonstrate the impact our work has, and we look forward to continuing to improve and protect the agency's programs and operations. While NARA is making efforts to improve in multiple areas, OIG products from this period highlight how NARA continues to struggle with various issues. Information Technology (IT) contracts need better administration, NARA's classified IT systems have multiple internal control weaknesses, the process for banning researchers needs improvement, and open audit recommendations need more attention. OIG investigators' efforts led to the conviction and sentencing of a researcher who stole World War II dog tags from NARA's holdings. Further, investigators also identified vulnerabilities in the report NARA used to monitor employee use of IT systems.

Finally, the new concentration on telework has exposed seams in the OIG's own IT resources where we depend on NARA. While this is discussed more thoroughly in the "Other Matters Affecting OIG Operations" section on page 6, it is important to note NARA is requesting funds to move the OIG to a more independent IT solution in fiscal year 2021. I thank NARA leadership for supporting the OIG in this endeavor, and for all of the agency's efforts to support the OIG mission and help improve NARA.

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 62nd 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. During the reporting period, the OIG issued the following audit reports and other non-audit reports concerning NARA programs and operations.[1] During this period the Office of Audits tracked $90,131,816 in questioned costs and $45,360,034 in funds to be put to better use.

Audits of Programs and Operations

- **Audit of NARA's Classified Information Systems.** NARA did not maintain proper Authorization-to-Operate (ATO) and lacks an effective Information Security Continuous Monitoring (ISCM) program for its classified systems. The ATOs for classified systems sampled were either severely outdated, or had not been issued at all. By not ensuring classified systems are properly authorized to operate based on a well-established continuous monitoring program, these systems may be at a significantly higher risk of containing unidentified security vulnerabilities, which could potentially allow unauthorized disclosure or misuse of national security-related information stored or processed on the systems. Additionally, we identified multiple internal control weaknesses in the management of NARA's classified systems. Specifically, integral components of Information System Contingency Planning (ISCP) were missing, a complete and accurate system inventory was not maintained, and proper physical and environmental controls were not always in place. As a result, NARA is hindered in its ability to identify and reduce the vulnerabilities and control failures associated with its classified systems, which potentially places the confidentiality, integrity, and availability of classified information at risk. (OIG Audit Report No. 20-AUD-03, dated December 12, 2019. See page 14.)

- **Audit of NARA's Oversight and Management of Information Technology Contracts.** NARA did not ensure effective implementation of acquisition management roles delegated to the Chief Acquisition Officer (CAO) in accordance with Services Acquisition Reform Act of 2003 (SARA). As a result, the CAO's role functioned as a supervisory Contracting Officer, and lacked the entity-wide governance of acquisition activities as required. Without comprehensive management of acquisition activities that ensures agency executives are making informed strategic decisions, NARA risks experiencing procurement challenges, such as contract costs overruns, duplicative projects, and poor contractor performance in a reactive instead of proactive manner. Additionally, NARA lacked a comprehensive acquisition career management (ACM) program that enhanced the acquisition workforce and provided for workforce planning,

[1] 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. All audits are posted online, while management alerts generally are not.

career paths, education, and training. Without an effective ACM program, NARA lacks assurance that its IT contracts are administered to deliver the best value possible to the agency. (OIG Audit Report No. 20-AUD-06, dated March 4, 2020. See page 14.)

- **Audit of NARA's Compliance Under the DATA Act of 2014.** NARA's fiscal year (FY) 2019, Quarter 1 submission was generally complete, accurate, and timely. Although the quality of NARA's data was substantially impacted by errors in data elements not attributable to NARA, our contractor found the quality of data to be of higher quality. The contractor also found that NARA implemented and used the Government-wide financial data standards established by OMB and Treasury. (OIG Audit Report No. 20-AUD-02, dated November 8, 2019. See page 15.)

Other Reports Concerning NARA Programs and Operations

- **Federal Information Security Modernization Act (FISMA) FY 2019 OIG Narrative.** NARA continued to stress their commitment to improving information security throughout the agency, and made steady progress to that end. NARA also continued to work to address open OIG audit recommendations related to its information security program. However, NARA needs to improve its identity and access management capability by 1) developing and implementing an identity, credential, and access management (ICAM) strategy; 2) ensuring privileged account reviews are conducted; and 3) ensuring the completion of system E-authentication risk assessments. (OIG Report No. 20-R-01, dated October 31, 2020. See page 16.)

- **NARA's Process for Banning Researchers from Facilities.** This Special Report examined the process NARA used to temporarily ban a researcher from NARA facilities. While it appeared NARA personnel earnestly tried to figure out a correct response a situation in accordance with agency procedures, the process used did not follow NARA's regulations and policy. There were several potential reasons for this, including references in the regulations to positions that no longer exist, and staff's incorrect use of the term "ban." We asked management to consider updating and clarifying NARA policy and regulations, and to ensure staff are trained on any updates. NARA agreed. (OIG Special Report NARA-SPEC-20-0075-S, dated February 4, 2020. See page 16.)

- **Compendium of Open Audit Recommendations to NARA.** As of September 30, 2019, NARA closed 114 of 346 total open recommendations identified at the beginning of FY 2019. However, it continues to be apparent the importance of closing open recommendations still varies among offices. Although NARA offices were given the opportunity to revise implementation dates in FY 2018, the majority of the offices exceeded their revised implementation dates and did not provide documentation supporting actions taken to support closure of the recommendations. (OIG Report No. 20-R-04, dated February 12, 2020. See page 17.)

- **Quarterly Open Recommendations Reports.** Every quarter the OIG issues reports to each NARA office summarizing their open audit recommendations, including data on new, closed, subsumed, and open audit recommendations at the end of the quarter. (OIG Report Nos. 20-R-05 and 20-R-07. See page 17.)

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, such as missing and stolen records. 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 other reports detailing specific issues or vulnerabilities we observe. Assessments are limited overviews of potential agency vulnerabilities used to alert management to issues and do not follow any set standards or procedures. The Inspector General has decided not to post these assessments online as they do not represent fully explored or detailed audit or investigative efforts. However, they are summarized in this report. These products contain observations, but do not include recommendations for corrective action. In this period, the OI received and reviewed 188 complaints and other intake actions, opened 4 new investigations, and closed 3 existing investigations.

The cost savings calculations attributed to OI work product for this period has totaled over $5,000. Cost savings include recoveries made as a result of investigations, including the appraised value of NARA holdings. Additionally, they include any identified misused agency resources and time, theft, and other monetary calculations identified during investigations. Time abuses are calculated as three years' worth of the offending behavior.

OI highlights for this reporting period include:

- 100 percent of our closed or completed investigations resulted in referrals for criminal, civil, and/or administrative action.
- A NARA researcher pleaded guilty to a Federal misdemeanor theft charge after we recovered four World War II military "dog tags," which we determined they stole from NARA. The researcher was sentenced to 18 months' probation and a $5,000 fine.
- A NARA employee received a seven day suspension after we determined they had not been honest and forthright about securing a Government-issued travel card, which was used by a family member to obtain unauthorized cash advances.
- In a Management Alert Report we identified vulnerabilities in a monthly report provided by the NARA Office of Information Technology, which is intended to provide data about employee misuse of NARA information technology. We identified the misuse report included false positive results and results influenced by malware, which was not properly detected or addressed. These issues undermined the accuracy of, and confidence in, the misuse report.

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 Protection Coordinator program, providing training and information to potential whistleblowers on various rules and protections available. This work included one-on-one consultations with individuals and working with other IG offices in the Federal community on various issues. In the next reporting period the Whistleblower Protection Coordinator plans to visit various NARA field offices to deliver in-person training and answer questions.

- Responded to multiple requests for OIG records under the Freedom of Information Act (FOIA).

- Provided substantial suggestions for improving multiple NARA issuances and ensuring they do not interfere with OIG independence. Some of the issuances reviewed included NARA 119 on institutional memberships, a supplement to NARA 802 on use and monitoring of NARA IT equipment and resources, and NARA 105 on NARA's visual identity.

- Responded to 17 requests from NARA for reviews of proposed legislation, Office of Management and Budget (OMB) regulations, congressional testimony, and other items.

Other Matters Affecting OIG Operations

Information Technology Independence Issues

The OIG has traditionally used NARA's information technology (IT) resources for our email and file storage needs. However, this is no longer efficiently meeting OIG IT needs while preserving our independence. For example, we learned NARA file searches for Freedom of Information Act (FOIA) requests and other searches actually examine the content of OIG emails because of the way the system is configured. This violates the confidentiality of whistleblowers and anyone who may contact the OIG via email. NARA's General Counsel has not provided any procedural way to fix this untenable situation, and supports the OIG moving to an independent email service. Since the OIG is a customer of NARA Information Services, NARA IT staff and NARA IT contractors may access OIG systems and data without any documentation of such access. While we have done what we can to get individuals to sign non-disclosure and confidentiality agreements, the fact these types of disclosures may happen puts OIG operations at risk. These issues have been magnified in this period due to NARA changing IT support contractors.

Further, NARA Information Services has the largest number of open audit recommendations, many of which point to NARA's IT security environment. Without independence in this area, the OIG is forced to bear all of NARA's IT and other vulnerabilities and risks, for which the OIG has no control. Some of these vulnerabilities are high and/or critical in nature, and in some cases exploitable. The current structure and reliance on NARA for IT services also hinders the OIG's ability to adhere to Federal IT policies, many of the same policies the OIG cites NARA for not adhering to. Finally, as a customer of Information Services and NARA's IT contractors, the OIG is subject to claims the OIG would not be independent or neutral if they had to investigate individuals working in these areas.

NARA has recognized the gravity of these issues, and is working with the OIG to investigate how we can move to a more independent and secure IT system to meet our operational needs. Any such project will require funding, and the additional funds necessary have been included in NARA's FY2021 budget request.

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 more than 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 hundreds of thousands of artifacts and hundreds of terabytes of electronic records. The number of records born and stored solely in the electronic world will only continue to grow; thus NARA developed the Electronic Record Archives to attempt to address this burgeoning issue.

NARA involves millions of people in its public programs, including exhibitions, tours, educational programs, film series, and genealogical workshops. In FY 2019, NARA reported more than 39 million online visits in addition to hosting over 4.0 million traditional visitors, all while responding to more than 1.2 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 (NHPRC), 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

In FY 2019, NARA was appropriated $391 million, including $373 million for operating expenses, $7.5 million for repairs and restoration of NARA-owned buildings, $6 million for the NHPRC, and $4.8 million for IG operations. At the end of the reporting period NARA was provided with an additional $8.1 million available until September 30, 2021, to address corona virus related issues under the CARES Act. With approximately 2,652 full-time equivalents (FTEs), NARA operates 44 facilities nationwide.

Introduction

About the Office of Inspector General (OIG)

The OIG Mission

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

Background

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

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

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

Resources

In FY 2019, Congress provided $4.8 million for the OIG's appropriation, including authorization for 24 FTEs. As in previous periods, the OIG budget is not at a level allowing us to effectively hire to our authorized FTE level. However, we were able to hire one new investigator, and one auditor hired last period reported for duty. At the close of the period the OIG had 21 FTEs on board, including an Inspector General, 11 FTEs devoted to audits, 7 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 reviewing CIGIE's legislative priorities, answering various data calls, monitoring legislation for developments of interest to the community, and developing input for proposed legislative actions.

CIGIE Audit Committee

The Audit Committee provides leadership to, and serves as a resource for, the Federal 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 the 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.

CIGIE Technology Committee Data Analytics Working Group (DAWG)

The OI and OA regularly attend and participate in the DAWG. The DAWG was created to assist IGs in acquiring tools and knowledge to better assess fraud, waste, and abuse within agency programs.

CIGIE Audit Peer Review Subcommittee (Appeals Process)

The AIGA serves on the Audit Peer Review Subcommittee's Review Report Appeals Process Group. This group receives OIGs' requests for the Audit Committee's Panels of Assistant Inspectors General for Audits' and IGs decision(s) on unresolved issues between OIGs.

CIGIE Training Institute

The OIG counsel continued to work with the CIGIE Training Institute. In this period OIG counsel taught IG criminal investigators at the Federal Law Enforcement Training Center (FLETC) and also briefed several new IGs on OIG related laws and authorities.

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.

CIGIE Enterprise Risk Management Working Group (ERMWG)

The OA regularly attends and participates in the ERMWG. The ERMWG contributes to the promotion and implementation of ERM principles in accordance with OMB Circular A-123 within the offices of the Inspectors General (OIG) community. OA is also a member of a subgroup with the ERMWG responsible for implementing an ERM Risk Assessment Approach for audit planning purposes.

CIGIE Technology Committee

The OA regularly attends and participate in the Technology Committee. The Technology Committee facilitates effective information technology (IT) audits, evaluations, and investigations by Inspectors General, and to provide a vehicle for the expression of the IG community's perspective on Government-wide IT operations.

CIGIE Technology Committee, Emerging Technology Subcommittee

The OA regularly attends and participates on the Emerging Technology Subcommittee. The Subcommittee reviews different emerging technologies employed by OIGs and how oversight is conducted over those activities, as well as how each OIG can use emerging technologies in its own work.

CIGIE Audit Committee, Internal Controls Working Group

The OA regularly attends and participates in the Internal Controls Working Group. The purpose of the Working Group is to reach a consensus on the 2018 Yellow Book Internal Control assessment and reporting requirements and further share lessons learned amongst/within the OIG community.

Oversight.gov Information Sharing

The OIG fully participates in oversight.gov, a CIGIE driven single source portal to search through reports of multiple OIGs.

CIGIE Federal Audit Executive Council (FAEC)

The OA regularly attends and participates in the FAEC. The FAEC discusses and coordinates issues affecting the Federal audit community with special emphasis on audit policy and operations of common interest to FAEC members

FAEC Audit Peer Review Guide Revision Working Group (Peer Review WG)

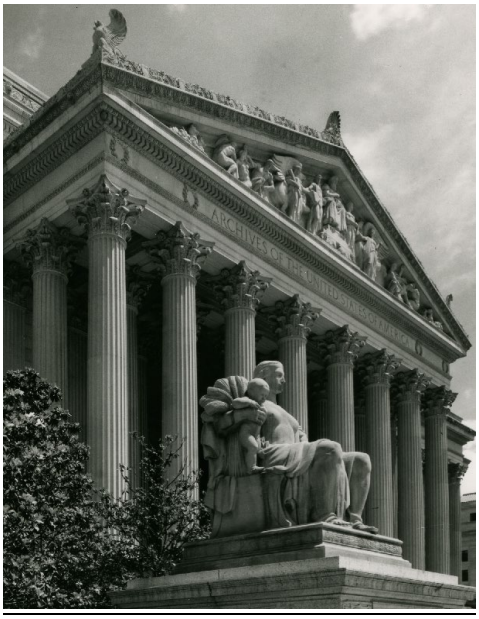
The OA regularly attends and participates in the FAEC Peer Review WG. The Peer Review WG updates the Audit Peer Review Guide, including updates related to the updated Yellow Book.

FAEC Digital Accountability and Transparency Act (DATA Act) Working Group

The OA regularly attends and participates in the DATA Act Working Group. The Working Group's mission is to assist the IG community in understanding and meeting its DATA Act oversight requirements by 1) serving as a working-level liaison with the Department of the Treasury (Treasury), 2) consulting with the Government Accountability Office (GAO), 3) developing a common approach and methodology, and 4) coordinating key communications with other stakeholders.

FAEC Financial Statement Audit Network

The OA regularly attends and participates with the FSAN. The FSAN was created to address financial statement audit issues that transcend individual Government agencies; and to discuss changes in accounting standards, auditing standards, laws and regulations that impact Federal financial statement audits.



Peer Review Information

Peer Review of NARA OIG's Audit Organization

The most recent peer review of the NARA OIG audit function was performed by the Federal Trade Commission OIG. In its report issued March 3, 2020, the NARA OIG received a peer review rating of pass for its system of quality control for the year ended September 30. 2019. Additionally, the OIG received no letter of comment. The next peer review of the OIG's audit function is scheduled for FY 2023.

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. The next investigative peer review was scheduled to be conducted by the Pension Benefit Guaranty Corporation OIG in spring 2020. However, due to the COVID-19 pandemic, the peer review has been delayed.

NARA OIG Peer Review of Other OIGs

The NARA OIG Office of Audits conducted a peer review of the Export-Import Bank (EXIM) of the United States for the period ending March 31, 2017. In this report, issued on September 8, 2017, the EXIM audit organization received a rating of pass for its system of quality control. The Office of Audits is scheduled to conduct a peer review of the Bureau of Governors of the Federal Reserve System and Bureau of Consumer Financial Protection for the period ending March 31, 2020.

Response to Congressional Items

The OIG continues to keep Congress informed about agency and OIG activities. The OIG actively worked with the CIGIE Legislation Committee and Congressional staff to review legislative priorities, provide comments on various pieces of potential legislation, and help communicate the views of CIGIE and the NARA OIG to relevant Congressional committees.

This reporting period these activities also included:

- Notifications of potential impacts of the COVID-19 pandemic on OIG operations.
- Responding to a letter from a Senator asking for information about various whistleblower issues at NARA.
- Beginning looking into an issue at NARA where an image was blurred to obscure certain words.
- Responding to a Senator's letter asking for information about NARAs actions concerning certain information requests.

Audit and Reports Overview

During this reporting period, the OIG issued three final audits and four other reports. These other reports include such things as Special Reports (which are used to convey information or issues to management officials without the technicalities of an 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:

- Cybersecurity Risk Management, determining whether NARA's classified systems are adequately managed and secured in accordance with Federal and NARA policies and guidelines.
- Controls over Loans of Holdings, determining whether proper controls are in place for loans of NARA holdings.
- Consolidated Audit of FY 2019 Financial Statements, rendering an opinion on whether NARA's consolidated financial statements are presented fairly in all material respects.
- Personnel Security and Suitability Program, evaluating controls over the adjudication of background investigations at NARA and determining if adjudication actions were completed timely and in accordance with policy.
- Travel Card Program, determining whether NARA's Travel Card Program has effective internal controls to safeguard against unauthorized use, abuse, and improper transactions not associated with official travel.
- Controls Over Use of IT Equipment and Resources, determining whether controls are adequate and effective to prevent and deter inappropriate use of the Internet on the government-assigned computing resources and mobile devices, as defined by NARA Directive 802, *Use and Monitoring of NARA Office and IT Equipment and Resources*
- High Value Assets (HVAs), determining whether NARA has controls in place to adequately protect its HVAs.
- Compliance with Fiscal Year 2019 Improper Payment Reporting Requirements, determining whether NARA is in compliance with the Improper Payments Information Act of 2002 (IPIA) as amended.
- Accountability for Actions Taken on Civil Rights Complaints, determining whether NARA processed discrimination complaints in a timely and efficient manner.
- Holdings Protection Program, determining whether NARA has controls in place to reasonably secure and protect holdings from theft or vandalism.
- Purchase Card Risk Assessment, assessing NARA's FY 2019 purchase card program due to unexplained difference in purchase card transactions in FY 2018 as noted in our FY 2018 Purchase Card Risk Assessment.
- NARA's Use of the 2017 Women's March Image, assessing the adequacy of internal controls over the exhibit development process.

Audit Summaries

Audit of NARA's Classified Information Systems

NARA has a longstanding material weakness in internal controls over information technology (IT) security as highlighted by previous OIG audits and the agency's financial reports. Consistent with the results of our previous audit, Audit of NARA's Classified Systems (OIG Audit Report No. 12-15, July 23, 2012), we again found classified systems were not adequately managed and secured.

NARA did not maintain proper Authorization-to-Operate (ATO) and lacks an effective Information Security Continuous Monitoring (ISCM) program for its classified systems. The ATOs for classified systems sampled were either severely outdated or had not been issued at all. This occurred because NARA is not adhering to National Institute of Standards and Technology (NIST) nor its own policy, that require ATOs to be issued and updated periodically. By not ensuring classified systems are properly authorized to operate based on a well-established continuous monitoring program, these systems may be at a significantly higher risk of containing unidentified security vulnerabilities, which could potentially allow unauthorized disclosure or misuse of national security-related information stored or processed on the systems.

Additionally, we identified multiple internal control weaknesses in the management of NARA's classified systems. Specifically, integral components of Information System Contingency Planning (ISCP) were missing; a complete and accurate system inventory was not maintained; and proper physical and environmental controls were not always in place. These conditions existed due to a general lack of management oversight and coordination by the Offices of Information Services and Business Support Services, as well as the system owners. As a result, NARA is hindered in its ability to identify and reduce the vulnerabilities and control failures associated with its classified systems, which potentially places the confidentiality, integrity, and availability of classified information at risk.

The report included twelve recommendations, which were intended to strengthen NARA's security controls for classified systems in order to protect the confidentiality, integrity, and availability of the systems and data, and also bring them to conformity with Federal and internal requirements and guidelines. (OIG Audit Report No. 20-AUD-03, dated December 12, 2019.)

Audit of NARA's Oversight and Management of IT Contracts

NARA has not ensured effective implementation of acquisition management roles delegated to the Chief Acquisition Officer (CAO) in accordance with the Services Acquisition Reform Act of 2003 (SARA). This occurred because executive management designed controls that weakened key authorities and responsibilities of the CAO, including exclusion of the CAO in advising and assisting the agency head and other agency officials to ensure NARA procurements supported the agency in achieving its mission. As a result, the CAO's role functioned as a supervisory Contracting Officer, and lacked the entity-wide governance of acquisition activities as required. Without comprehensive management of acquisition activities that ensures agency executives are making informed strategic decisions, NARA risks experiencing procurement challenges, such as

contract costs overruns, duplicative projects, and poor contractor performance in a reactive instead of proactive manner.

In addition, NARA lacks a comprehensive acquisition career management (ACM) program that enhanced the acquisition workforce and provided for workforce planning, career paths and education and training. Specifically, we found:

• CORs assigned to NARA's most complex and critical IT contracts lacked appropriate certifications,
• training requirements for CORs did not comply with federal guidelines, and
• NARA's program/project manager certification program operated under outdated guidance.

This occurred because the CAO did not establish and maintain acquisition management controls in accordance with Federal policies. During FY 2017 and FY 2018, NARA spent over $90 million in contracting for major IT investments. However, CORs assigned to these contracts did not meet the appropriate training and experience levels. Without an effective ACM program, NARA lacks assurance that its IT contracts are administered to deliver the best value possible to the agency.

The report included seven recommendations, which were intended to strengthen the oversight of the Office of the Chief Acquisition Officer, improve management of the Contracting Officer's Representative (COR) workforce, and strengthen implementation of the Federal Acquisition Certification Program for Program and Project Managers. (OIG Audit Report No. 20-AUD-06, dated March 4, 2020.)

Audit of NARA's Compliance Under the DATA Act of 2014

We contracted with an independent certified public accounting firm to conduct a performance audit of NARA's compliance with the DATA Act. The audit's objectives were to assess 1) the completeness, accuracy, timeliness, and quality of NARA's fiscal year (FY) 2019 first quarter financial and award data submitted for publication on USASpending.gov, and 2) NARA's implementation and use of the Government-wide financial data standards established by the Office of Management and Budget (OMB) and the U.S. Department of the Treasury (Treasury).

Our contractor found that NARA's FY 2019 Quarter 1 submission was generally complete, accurate, and timely. Although the quality of NARA's data was substantially impacted by errors in data elements not attributable to NARA, the contractor found the quality of data to be of "higher quality." They also found that NARA implemented and used the Government-wide financial data standards established by OMB and Treasury.

The report made two recommendations, which were intended to strengthen controls over data sent to the Federal Procurement Data System. (OIG Audit Report No. 20-AUD-02, dated November 8, 2019.)

Summaries of Other Reports

Federal Information Security Modernization Act (FISMA) FY 2019 OIG Narrative

NARA continues to stress their commitment to improving information security throughout the agency, and is making steady progress to that end. NARA also continues to work to address open OIG audit recommendations related to its information security program. NARA made several noteworthy improvements during FY 2019 throughout the domain areas, which have been recognized in the IG metric responses as relevant and applicable:

- Through the addition of Information System Security Officers (ISSOs), NARA's development and maintenance of system security documentation generally improved.
- NARA broadened its identification of risks by improving its Risk Management Framework (RMF) Dashboard to incorporate more systems.
- NARA improved its system inventory reporting.

To fully progress towards the "consistently implemented" maturity model level, NARA needs to improve its identity and access management capability by 1) developing and implementing an ICAM strategy; 2) ensuring privileged account reviews are conducted; and 3) ensuring the completion of system E-authentication risk assessments.

In addition, NARA also needs to provide better management oversight and follow up to ensure training is completed and documented by required individuals in a timely manner and work to improve its contingency planning function to ensure it completes and tests its system-level contingency plans, conducts system Business Impact Analyses (BIAs), and establish contingency planning strategies for cloud systems. (OIG Report No. 20-R-01, dated October 31, 2019.)

NARA's Process for Banning Researchers from Facilities

This Special Report examined the process NARA used to temporarily ban a researcher from NARA facilities after an alleged incident. This limited review did not examine the alleged conduct or make any determination surrounding it, and was limited to NARA's process alone. It appeared all NARA personnel were earnestly trying to figure out a correct response to the situation in accordance with agency procedures. However, the term "ban" seemed to be used synonymously with both removal and the revocation of research privileges. These are different steps available to address issues in the research room, and this confusion of terms led NARA to issue a ban without following all terms of NARA policy and published regulations. Further, NARA policy and regulations reference employee titles which are no longer used, leading to issues surrounding who is able to ban a researcher. Accordingly, in the instance reviewed, NARA's process for banning researchers did not function effectively in accordance with NARA policy and regulations. We asked management to consider updating and clarifying NARA policy and regulations, and to ensure staff are trained on any updates. NARA agreed. (OIG Special Report NARA-SPEC-20-0075-S, dated February 4, 2020.)

Compendium of Open Audit Recommendations to NARA

As of September 30, 2019, NARA closed 114 of 346 total open recommendations identified at the beginning of FY 2019. However, it continues to be apparent that the importance of closing open recommendations still varies among offices. Although NARA offices were given the opportunity to revise implementation dates in FY 2018, the majority of the offices exceeded their revised implementation dates and did not provide documentation supporting actions taken to support closure of the recommendations.

Based on the documentation received, the Office of the Chief Financial Officer (CFO Office) has not made closing open recommendations a priority. In FY 2019, the CFO Office subsumed one, and closed three, open recommendations. As of September 30, 2019, the CFO Office still had 28 open recommendations resulting from audits conducted between FY 2013 through FY 2019. Since issuance of the associated audit reports, the CFO Office has not provided any documentation to the OIG in an effort to close 20 of these recommendations although revised implementation dates were granted in FY 2018. There has also been no communication with the OIG in addressing these open recommendations, many of which pointed to internal controls. Without maintainable action plan dates NARA will continue to face a mounting list of open recommendations that are well beyond the years when they were first identified. Additionally, without implementation of the recommendations, NARA continues to lack internal controls in many of its program areas.

We will continue to meet our responsibilities as required for audit follow-up, and look forward to working with NARA management in their efforts to implement corrective actions that will help reduce the number of open recommendations. (OIG Report No. 20-R-04, dated February 12, 2020.)

2020 Quarterly Open Recommendations Reports

At the end of every quarter the OIG issues reports to each NARA office summarizing their open audit recommendations, including data on new, closed, subsumed, and open audit recommendations. These reports are intended to ensure closing open audit recommendations remain a priority and NARA senior managers are aware of the outstanding audit issues in their respective areas in order to expedite efforts towards addressing the recommendations. (OIG Report Nos. 20-R-05 and 20-R-07.)

Investigations Overview

The 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, such as missing and stolen records. 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 as discussed earlier in this report. Their purpose is to alert management to issues. While they may offer potential suggestions, the IG has decided they do not make recommendations for corrective action and they are not generally posted online.

Significant Investigations and Updates

Status of Previously Reported Investigations:

Stolen Military Identification "Dog Tags" Recovered

As previously reported, the OI investigated several American servicemen's military identification "dog tags" from World War II-era records stolen from NARA by a researcher. In April 2019, the OI executed several search warrants, leading to the recovery of the stolen dog tags. The OI interviewed the researcher, who admitted to stealing the dog tags. In May 2019, the OI arrested the researcher, and they were charged in the U.S. District Court for the District of Maryland with one count of misdemeanor theft. In November 2019, the researcher pleaded guilty and, in January 2020, was sentenced to 18 months' probation and a $5,000 fine.

Misuse of Travel Credit Card

As previously reported, the OI investigated a NARA employee whose Government-issued travel card was used to obtain unauthorized cash advances in identical amounts, two months in a row. At the time of the first cash advance, the employee explained a family member had inadvertently used the Government travel card instead of a personal credit card to withdraw cash for the employee before an official work trip that was later canceled. The employee was required to re-take travel card training, secure the Government travel card, and pay the value of the cash advance. After the second cash advance, the employee claimed a different family member had used the card without permission. The investigation revealed the employee had not secured the card, the initial family member had used the card on both occasions for personal withdrawals, and the employee had not been honest and forthright in their explanations. The United States Attorney's Office declined criminal prosecution. The OI reported the results to NARA management to determine whether corrective action may be warranted. In this reporting period, the employee received administrative discipline.

Theft of Historic Photographic Prints

As previously reported, five World War II-era photographic prints from NARA's collection were discovered for sale at a public auction house. The OI stopped the auction, obtained the prints, and determined they were part of NARA's archival collection of original Dorothea Lange

photographs. The investigation traced the documents to a private collector, who led the OI to believe they still possessed potentially substantial quantities of NARA records. In September 2018, the OI obtained and, in conjunction with the Library of Congress Office of Inspector General, executed a Federal search warrant on the collector's residence, seizing hundreds of additional photographs. The private collector was determined to be an innocent third party who purchased the stolen items. During this reporting period, the matter was declined by the United States Attorney's Office for criminal prosecution. NARA subject matter experts evaluated all of the seized materials, and reclaimed the photographs missing from NARA's collection. All items belonging to non-NARA institutions (e.g., the Library of Congress) were restored to those institutions, and the remainder of the seized items were returned to the innocent private collector.

Open and Completed Significant Investigations:

Undeclared Outside Employment and Time and Attendance Fraud

The OI received allegations that an employee was engaged in a multifaceted time and attendance fraud involving telework abuse, inappropriate claims for credit hours, engaged in unreported outside employment, and conducted outside employment during the same time they claimed to be on official NARA duty. The investigation substantiated the allegations that the employee had undeclared outside employment for which they performed substantial quantities of work over many months during times which may have overlapped their NARA working hours. The investigation also uncovered multiple time and attendance issues, including timesheets with irregular credit hours, which were approved by supervisors despite violating NARA policy. The United States Attorney's Office declined criminal prosecution. The results of the investigation were provided to management to determine whether corrective action may be warranted.

Employee Bomb Threat Posted on Personal *Facebook* Page

The OI investigated allegations that a NARA employee expressed appreciation for "the desire to blow up the Archives" on their personal *Facebook* page. Additionally, several other NARA employees and the employee's supervisor "liked" the posting. The OI took swift action and determined there was no active threat. The investigation revealed that the employee made the comment as a reference to a movie after consuming alcohol, and during a frustrating workweek, but had no real intent to commit any act of violence. The employee, who had deleted the posting, acknowledged wrongdoing and apologized. They consented to a search of their workplace, which did not reveal anything dangerous or threatening. The OI also coordinated with the Security Management Division, who placed the employee into a security status requiring them to undergo enhanced security screening when entering NARA facilities. NARA also sent an agency-wide communication to employees concerning threats to NARA facilities. The United States Attorney's Office declined criminal prosecution. Potential administrative action is pending.

Misuse of Position for Personal Gain

The OI received allegations that a NARA supervisor:

- repeatedly used their personal credit card to make office-related purchases, and was then being reimbursed, in order to benefit from the purchase points and airline miles;
- consistently favored a particular vendor in violation of procurement regulations; and

- engaged in retaliation against a whistleblower employee who reported the alleged misconduct.

The investigation determined that:

- with management's approval the supervisor used their personal credit card for office-related purchases, earning personal benefits (e.g., airline miles) associated with the purchases, but there was neither a practical alternative to doing so, nor was there relevant guidance to address the specific circumstances;
- the supervisor was not steering contracts to the named vendor in violation of procurement regulations;
- the supervisor imposed a performance based action against the employee shortly after the employee made their report, but it was not an act of whistleblower retaliation.

The reporting employee had a documented history of performance issues, and the process for employee discipline had been initiated well in advance of the employee's report. The process was coordinated with the Office of Human Capital, but the action was not finalized and imposed until after the employee made their report. The specific circumstances which resulted in the supervisor using their personal credit card have been reviewed by NARA's Office of General Counsel, and an appropriate alternative process has been created.

Local Nuisance Barred from Ford Museum

The OI initiated an investigation after multiple reports alleging an individual was harassing employees at the Gerald Ford Museum, and employees feared for their safety. The individual was previously considered a nuisance, but had infrequent contact with the museum. However, they were increasingly calling and visiting the museum, and having emotionally uncontrollable and delusional outbursts alleging to be the real child of former President Gerald Ford. The individual was also calling employees and leaving obscene and hostile messages for staff, which escalated in frequency and emotional intensity to the point it was disrupting museum operations and creating a concern the individual was on a trajectory to become violent. The OI coordinated with the United States Secret Service, who conducted a threat assessment of the individual. The investigation revealed the individual had a long history of court-mandated psychiatric evaluation and treatment, and was recently not compliant with their treatment. During the course of the investigation, the individual was ordered to receive in-custody psychiatric evaluation and treatment for an undisclosed prolonged period. The OI also learned that the individual had a weapons violation in the past, and collaborated with museum staff and local law enforcement to enact a court-enforceable ban of the individual from all NARA property. The United States Attorney's Office declined criminal prosecution.

Use of Controlled Substance at Work

The OI received an allegation that a NARA employee had come to the office on several occasions smelling of marijuana. The investigation did not find evidence that the employee was using marijuana. Investigators made several covert visits to the employee's office, and did not detect the odor of marijuana on any visit. Additionally, the employee passed a urinalysis drug test, and denied using marijuana.

Violation of the Procurement Integrity Act

The OI received an allegation a NARA employee provided privileged contract-related information to a representative of one of NARA's contract companies that would potentially

participate in a bid for an additional upcoming contract. The investigation did not find evidence that the employee provided privileged procurement information to the contractor. Furthermore, the OI determined the procurement information the employee was privy to was unlikely to result in an unfair advantage to a vendor. Additionally, the employee's supervisor provided guidance concerning the employee's conduct around contractors, which included avoiding giving the appearance of impropriety.

Time and Attendance Fraud

The OI investigated allegations that a NARA employee spent significant quantities of their working hours in the morning watching *YouTube* videos, and often disappeared from the office in the afternoons. The investigation determined the allegations were unsubstantiated. There had been a single previous incident where the employee was counseled for watching videos in the office. The employee's supervisor had subsequently been alert for repeat violations, and reported there were none. The investigation also revealed that, one day per week, the employee used their break time to conduct a family-related task at home. The employee's supervisor was aware of this activity and approved it, noting that the employee lived so close to workplace the activity did not impact the employee's work or exceed their allowable break time. The OI conducted covert spot-checks at different times of day, which consistently showed the employee working at their desk.

Investigations of Senior Government Employees[2]

Supervisor Pressured Employee to Withdraw Application

The OI investigated an allegation that an employee was pressured by their supervisor to withdraw their application for a promotion. During the investigation, the supervisor denied the allegation, and the employee acknowledged the supervisor had not demanded or requested that the employee withdraw their application. The investigation concluded the employee had voluntarily withdrawn their application, and the allegation the supervisor had engaged in a prohibited personnel practice could not be substantiated.

Significant Referrals

Employee Terminated for Failing Periodic Security Suitability Review

The OI administratively referred an allegation that a NARA employee failed their periodic security suitability review due to debt, noncooperation with the security inquiry, and submission of false information. On confirmation of the allegations and compliance with appropriate procedures, NARA terminated the person's employment.

Contract Employee Terminated After Confrontation with Security Staff

The OI administratively referred an allegation that an employee of a NARA contract company disregarded security exit protocols and was abusive to security staff when called back. On confirmation of the allegations, and determination that the contract employee had a history of

[2] A senior government employee is defined as anyone occupying a position classified at or above GS-15, or for those not on the General Schedule, whose rate of basic pay is equal to or greater than 120% of the GS-15 minimum.

aggressive interactions with security staff, the contract company terminated the person's employment.

Oversight

Review of Ongoing Vulnerabilities in Reports of Employee Abuse of Agency Information Technology Resources

The OI issued a Management Alert Report (the Report) identifying ongoing vulnerabilities in and limitations to the agency's monthly Inappropriate Use Report (the IUR), which attempts to capture several different types of employee abuse of information technology resources throughout the agency, such as streaming video and viewing pornographic images. The Report identified that the IUR included false positive results, and results influenced by malware that were not properly detected or addressed. These conditions undermine the accuracy of, and confidence in, the IUR, rendering it largely unusable for the purpose for which it is generated. NARA management responded they would not take any action pending their receipt and review of a related audit being conducted by the OIG's Office of Audits.

Review of Access to Special Holdings at Two Presidential Libraries

As previously reported, the OI conducted a limited assessment of compliance with appropriate regulations regarding unescorted access to specially-protected holdings at two Presidential libraries. NARA policy restricts unescorted employee access to the Presidential libraries' specially-protected holdings to those who have security clearances, and to those who have passed a security check adjudicated by the NARA Security Management Division. Both Presidential libraries were in compliance with their understanding and application of the appropriate regulations. However, the Security Management Division did not have complete paperwork for every cleared employee, and the name of one employee who had been censured for having a lower-than-acceptable credit score remained on the Presidential library's list of cleared employees instead of being removed pending re-adjudication. The assessment was forwarded to NARA administration for review and appropriate action. During this reporting period, NARA administration determined that they would not pursue credit checks on the employees.

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	188
Hotline and Complaints referred to NARA or another entity	44

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*.

Top Ten Management Challenges

Each year, Federal Inspectors General are required to identify and report on the top challenges facing their respective agencies. The most significant management and performance challenges facing NARA are based on legislative mandates and our experience and observations from our oversight work. We conduct independent audits, investigations, and other reviews in order to make NARA a better agency, hold people accountable, and prevent problems before they happen. To fulfill this mission, we focus our oversight work on areas we believe represent the agency's most significant challenges. Here are NARA's top ten management challenges.

1. Electronic Records Archives

Electronic records are the future of government archiving, and the vast volumes of electronic records that will need to be preserved are simply staggering. NARA's plan to tackle this mission critical issue is the Electronic Records Archives (ERA) system. Initially billed as a solution for storing files in any format for indefinite future access, the program has been fraught with delays, cost overruns, funding shortfalls, and technical short-comings virtually since inception. As a result, many core requirements from initial plans have never been addressed, and the ERA lacks the capabilities originally envisioned. ERA faces many challenges going forward, including the predicted massive growth in the amount and diversity of digital materials NARA will have to preserve. This is coming at the same time stakeholders expect expanded capabilities, such as online access and searching, that drive openness and cultivate public participation.

The ERA is a "system of systems," with the ERA Base System the main point for receiving and storing records from Federal agencies. NARA has recognized problems with the ERA Base System's reliability, scalability, usability, and costs have prevented it from being adequate for NARA's current and expected future workload. These problems, combined with advances in technology (particularly cloud computing), led NARA to determine it is essential to evolve the ERA Base System. This will allow NARA to fix and re-factor current capabilities, as well as adapt and expand new capabilities to meet the expected demands of a rapidly growing backlog of digital material. Named ERA 2.0, this is an on-going development effort with limited implementation and estimated lifecycle costs of $86 million. The ERA 2.0 timeline continues to slip, with the component slated to subsume the old ERA Base expected in early FY 2021 and a classified instance not arriving until at least FY 2024. Some components of ERA 2.0 have been put into production and are used by a number of NARA custodial staff who work with digital materials. However, until ERA 2.0's functionality is put into full production, the current ERA's longstanding deficiencies may continue to impact NARA.

2. Improving Records Management

While the ERA system is intended to handle electronic records received by NARA, the agency needs to ensure the proper electronic and traditional records are in fact preserved and sent to NARA in the first place. NARA must work with Federal agencies to ensure proper appraisal, scheduling, and transfer of permanent records in all formats. The major challenge is how best to accomplish this in a rapidly changing technological environment.

The Office of Management and Budget (OMB) M-19-21, *Transition to Electronic Records*, establishes new goals for electronic recordkeeping to support government-wide efforts to transition to a fully electronic (paperless) Government. M-19-21 directs agencies to

manage *all* of their permanent records in electronic format by December 31, 2022. Agencies are also required to:

1) convert all temporary records to electronic format or store them in commercial storage facilities after December 31, 2022,
2) continue to manage email records in electronic format and continue efforts to manage permanent *electronic* records electronically by December 31, 2019 (both of these goals were established in 2012),
3) manage all permanent records electronically *and with appropriate metadata* – that meets NARA standards – by 2022, and
4) either stop producing temporary records in analog formats by 2022 or prepare to store future temporary records in commercial facilities.

M-19-21 also directs agencies who operate their own records storage facilities to transfer their records to the Federal Records Centers Program or a commercial storage facility and close their agency-owned facilities by December 31, 2022.

NARA and the rest of the government is challenged with meeting these deadlines while determining how best to manage electronic records and make e-Government work more effectively.

3. Information Technology (IT) Security

NARA's challenges in IT Security continue to mount against the agency's goals to accomplish its mission as the nation's record keeper. Over the past decade, annual Federal Information Security Modernization Act (FISMA) assessments have consistently identified areas in need of significant improvement. NARA labeled IT Security a "material weakness" under the Federal Managers' Financial Integrity Act (FMFIA) from 2007 to 2019 with exceptions in 2013 and 2014, when it was considered a "reportable issue." While management has developed an action plan to resolve identified control deficiencies, NARA does not expect to fully implement it until FY 2023.

Many of NARA's issues stem from control weaknesses which contribute to underdeveloped or ineffectively implemented policies, and the Chief Information Officer's (CIO's) lack of insight into NARA's overall IT architecture and security. Further, NARA's IT systems oftentimes bypass the formal security assessment and authorization requirements before commencing operations, putting data security and system functionality at risk. Adding to the challenge, the CIO does not report directly to the agency head. These conditions cause current security and performance problems, and inhibit NARA from effectively establishing a strategy for the next generation of NARA's network.

While NARA has introduced initiatives to promote a mature program, real progress will not be made until NARA establishes an effective system of internal control for information security. NARA's mission relies on the confidentiality, integrity, and availability of our electronic records and IT systems. NARA must ensure the security of its data and systems or risk undermining the agency's credibility and ability to carry out its mission.

4. Expanding Public Access to Records

Records that cannot be accessed have little use, and the public expects more and more records to be online. NARA's strategic goal to "Make Access Happen" affirms public access as NARA's core purpose, and NARA has committed to digitize the nation's archives and make them available online. This goal is a massive undertaking involving billions of pages, films and photographic media, and other records. However, NARA's historic digitization approaches were not large enough to make significant progress. Other attempts have had issues as well. For example, poor planning and system limitations kept millions of records digitized by NARA partners from being 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 an effective digitization strategy and expand public access to records.

At a basic level, in order to "Make Access Happen" NARA must gain physical and intellectual control over its holdings. That is, NARA must physically control the records and know what they are. This initial step is referred to as archival processing. However, approximately 20 percent of NARA's textual holdings (by series) have not been processed, so the public does not have efficient and effective access to them. Thus, the agency has begun an initiative to accelerate archival processing to increase the records available for research. 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. This work includes standardizing processing procedures across the agency, strengthening internal controls, and monitoring performance.

5. Meeting Storage Needs of Growing Quantities of Records

NARA is running out of room and is challenged in acquiring sufficient archival space to store its current volume of textual records. Even with the rise of electronic records and the requirements of M-19-21, Transition to Electronic Records, there are still decades worth of paper records still scheduled to come to NARA. Currently space limitations affect NARA's accessioning, processing, preservation, and other internal efforts. By law, the Archivist is responsible for the custody, control, operation, and protection of NARA's buildings used for the storage of Federal records. NARA regulations require these facilities to meet certain physical and environmental requirements. Without additional space, NARA may have to house historical records in space not meeting its own requirements. The challenge is to ensure NARA's and other agencies' facilities comply with NARA regulations or to effectively mitigate risks to records stored in sub-standard facilities.

Additionally, the agency is also challenged to meet data storage requirements for electronic records. NARA's in-house data storage is reaching capacity, impacting the agency's digitization efforts and other IT programs. Increasing amounts of electronic data storage are necessary for NARA to meet its mission. Without adequate storage, NARA cannot continue accepting, storing, and processing electronic records or make them available to the public. NARA is challenged to develop an enduring enterprise-wide data storage management solution appropriate for handling the nation's history while complying with OMB's Federal Data Center Consolidation Initiative, which focuses on reducing the energy and real estate footprint.

6. Preservation Needs of Records

Every day NARA's holdings age and slowly degrade. This is true for all records, not just paper, as time affects the physical media electronic and audiovisual records are stored on as well. Further, as computer programs become obsolete, the records stored in those formats may become impossible to use. 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. NARA's new Preservation Strategy (2019–2022) emerged from the findings of an FY 2018 Preservation Programs internal review. The aim of the review was to critically evaluate preservation needs across NARA with a view to recommending how Preservation Programs can meet the challenges facing NARA now and in the future. The review identified many issues that needed consideration, including: supporting the delivery of increasing volumes of electronic records to the American public online (NARA's Strategic Goal 1); climate instability, which will require reassessing how NARA preserves its holdings; and working with fixed or reduced resources. Without action, pieces of the unique history of America will be lost.

7. Improving Project and Contract Management

NARA faces significant challenges concerning project and contract management. For example, there have been cost and schedule overruns, contract requirements are not always well defined, large dollar IT contracts have lacked adequate oversight, contractor performance is not consistently evaluated and reported, and IT projects are not always carried out in accordance with guidelines. This affects whether or not NARA obtains the right goods and services at the right price. NARA is challenged with instilling the proper management structure, function, coordination, and visibility to adequately align acquisition functions with NARA's mission and needs. A significant part of this challenge is NARA's acquisition workforce. Strengthening the acquisition workforce is essential to improving contractor management and oversight. However, NARA does not effectively identify and track the agency's acquisition workforce, or coordinate with program areas when designating CORs. This has led to using CORs without proper certifications. NARA is challenged to strengthen internal controls over acquisition functions and provide better oversight and management of its procurement activities to ensure it effectively and efficiently adheres to Federal and internal guidance.

The OIG has encountered multiple examples of project management issues. For example, NARA relied on end-of-life servers, hindering IT modernization efforts. Further, NARA did not document briefings to its senior management oversight group during the development of NARA's largest IT project, the ERA system, and there is little evidence the group identified or took appropriate corrective actions. However, NARA spent more than $23 million and 3.5 years developing solutions to correct deficiencies in the ERA Base System. Its successor, the ERA 2.0 project, continued to experience challenges including funding and aligning with NARA's System Development Life Cycle (SDLC) policy. Additionally, despite spending approximately $2.8 million over the past 12 years, NARA has not fully implemented all of the requirements in Homeland Security Presidential Directive-12. The GAO also reported NARA inconsistently used 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 disciplines like EVM limits NARA's ability to effectively manage projects and accurately

report on their progress.

8. Physical and Holdings Security

People continue to steal documents and artifacts from NARA for their monetary and historical value. Further, the priceless history represented in these records is threatened by fire and other man-made and natural disasters. Yet the threats do not stop there as NARA holds troves of national security information as well. NARA must ensure the safety and security of people and records in our facilities. NARA's security posture has improved with the implementation of the Holdings Protection Team and stricter access controls. However, NARA's challenge is to run an effective Holdings Protection Program in an environment where new threats emerge and adversaries are continuously adapting.

9. Human Resources Management

NARA's employees are the backbone of the agency, and one of NARA's strategic goals is to "build our future through our people." In May 2019, NARA completed the migration of staffing, classification, employee benefits, and workers' compensation functions to the Department of Treasury, Bureau of the Fiscal Service, Administrative Resource Center (ARC). NARA is challenged to correct past deficiencies in Human Capital practices, including HR data and electronic Official Personnel Folders (eOPF), to enable support of NARA's mission. NARA's ability to attract, recruit, and retain employees is critical to many of the other top management challenges, but NARA continues to lack adequate policies and procedures making it difficult to manage human capital effectively and efficiently.

10. Enterprise Risk Management

OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control is designed to ensure Federal managers effectively manage risks. It does this by implementing Enterprise Risk Management (ERM) practices and 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.

However, NARA management has not made ERM a strategic priority and has yet to implement an ERM program that clearly identifies, prioritizes, and manages risks. 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. 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 might not clearly reflect NARA's current internal control environment, including risks. NARA's challenge is to ensure the agency complies with the requirements of OMB Circular A-123, and develops and fully implements an ERM capability to effectively identify, manage, and mitigate critical agency risks.

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, 12
§ 5(a)(1)	Significant problems, abuses, and deficiencies discovered during the reporting period	2–4, 14–22
§ 5(a)(2)	Significant recommendations for corrective action	2–4, 14–16, 34–36
§ 5(a)(3)	Prior significant recommendations on which corrective action has not been completed	34–36
§ 5(a)(4)	Summary of prosecutorial referrals and convictions	18–21, 30
§ 5(a)(5)	Information or assistance refused and reported to agency head	33
§ 5(a)(6)	List of audit, inspection, and evaluation reports issued	31
§ 5(a)(7)	Summaries of significant reports	2–4, 14–22
§ 5(a)(8)	Questioned costs in audits, inspections, and evaluations	31
§ 5(a)(9)	Funds put to better use in audits, inspections, and evaluations	32
§ 5(a)(10)	Prior audit, inspection, and evaluation reports with no management decision, no management comment, or unimplemented recommendations	34–36
§ 5(a)(11)	Significant revised management decisions	33
§ 5(a)(12)	Significant management decisions with which the OIG disagreed	33
§§ 5(a)(14), (15), (16)	Reporting on OIG peer review	12
§ 5(a)(17)	Statistical table on investigations and referrals	30
§ 5(a)(18)	Description of metrics used in § 5(a)(17) table	30
§ 5(a)(19)	Reporting on substantiated investigations of senior government employees	None this period (see pg 21)
§ 5(a)(20)	Reporting on substantiated whistleblower retaliations	33
§ 5(a)(21)	Reporting on agency attempts to interfere with OIG independence	33
§ 5(a)(22)(A)	Closed inspections, evaluations, and audits not disclosed to the public	33
§ 5(a)(22)(B)	Closed investigations of senior government employees not disclosed to the public	21
P.L. 110-181	Annex on completed contract audit reports	32
P.L. 104-106	Open audit recommendations	34–36

SUMMARY OF INVESTIGATIONS AND PROSECUTORIAL REFERRALS

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

Investigative Workload	
Hotline and complaints received and opened this reporting period	188
Hotlines and complaints referred to other parties during this reporting period	44
Investigations opened this reporting period	4
Investigations closed this reporting period	3
Investigative reports issued this reporting period	2
Investigative Results	
Total individuals referred to DOJ for prosecution	5
Individuals referred to DOJ – accepted for prosecution	1
Individuals referred to DOJ – declined for prosecution	5
Individuals referred DOJ – pending prosecution decision	0
Total individuals referred to state and local authorities for prosecution	0
Individuals referred to state and local authorities – accepted for prosecution	0
Individuals referred to state and local authorities – declined for prosecution	0
Individuals referred state and local authorities – pending prosecution decision	0
Arrest	0
Indictments and information	0
Convictions	1
Fines, restitutions, judgments, and other civil and administrative recoveries	$5,025
Administrative Remedies	
Employee(s) terminated	1
Employee(s) resigned	0
Employee(s) suspended	0
Employee(s) given letter of reprimand or warnings/counseled	1
Employee(s) taking a reduction in grade in lieu of administrative action	0
Contractor (s) removed	1
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
20-AUD-02	Compliance with Digital Accountability and Transparency Act of 2014	11/8/2019	$0	$0	$0
20-AUD-03	Classified Information Systems	12/12/2019	$0	$0	$0
20-AUD-06	Oversight and Management of Information Technology Contracts	3/4/2020	$90,000,000	$0	$0

LIST OF OTHER REPORTS ISSUED

Report No.	Title	Date
20-R-01	FY 2019 FISMA Narrative	10/31/2019
20-R-04	Compendium of Open Audit Recommendations to NARA	2/12/2020
20-R-05	2020 1st Quarter Open Recommendations Report	2/13/2020
20-R-07	2020 2nd Quarter Open Recommendations Report	3/31/2020

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	1	$131,816	$0
B. Which were issued during the reporting period	1	$90,000,000	$0
Subtotals (A + B)	2	$90,131,816	$0
C. For which a management decision has been made during the reporting period	1	$90,000,000	$0
(i) dollar value of disallowed cost	0	$0	$0
(ii) dollar value of costs not disallowed	1	$90,000,000	$0
D. For which no management decision has been made by the end of the reporting period	1	$131,816	$0
E. For which no management decision was made within 6 months	1	$131,816	$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)	2	$45,360,034
B. Which were issued during the reporting period	0	$0
Subtotals (A + B)	2	$45,360,034
C. For which a management decision has been made during the reporting period	0	$0
(i) dollar value of recommendations that were agreed to by management	0	$0
Based on proposed management action	0	$0
Based on proposed legislative action	0	$0
(ii) dollar value of recommendations that were not agreed to by management	0	$0
D. For which no management decision has been made by the end of the reporting period	2	$45,360,034
E. For which no management decision was made within 6 months of issuance	2	$45,360,034

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 contracts during this period, they were generally program audits as opposed to contract audits.

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	None.
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.
5(a)(22)	Closed inspections, evaluations, and audits not disclosed to the public	All closed audits were disclosed to the public, other products which were not are summarized throughout this report.

Reporting Requirements

SUMMARY OF OPEN AUDIT RECOMMENDATIONS

An important responsibility of the OIG is to follow-up on previous issued reports with outstanding recommendations. During this period, 22 audit recommendations were closed and the agency accepted the risk on one recommendation. At the close of the period, there were 291 total open recommendations.

Report Number	Date Issued	Title	Number of Open Recommendations
09-15	9/29/2009	Work at Home System	1
10-04	4/2/2010	Oversight of Electronic Records Management in the Federal Government	1
11-02	11/8/2010	Network Vulnerability and Penetration Testing	2
12-09	5/10/2012	Data Center Consolidation Initiative	5
12-10	9/13/2012	Follow-up Review of OIG Audit Report 08-01: Audit of the Process of Safeguarding and Accounting for Presidential Library Artifacts	5
12-11	8/27/2012	Network Discovery and Assessment	4
12-15	7/23/2012	Classified Systems	3
13-01	12/10/2012	Internal Controls Program	1
13-08	7/9/2013	Preservation Program (Textual)	8
13-10	7/9/2013	Archival Facilities	5
13-11	9/19/2013	Base ERA's Ability to Ingest Records	2
13-14	9/18/2013	Processing of Textual Records	2
14-01	1/30/2014	Management and Oversight of NARA's Energy Savings Performance Contracts (ESPCs)	1
14-08	4/17/2014	Capital Planning and Investment Control (CPIC) Process	7
14-10	5/9/2014	Enterprise Wireless Access	3
15-02	11/12/2014	Mobile Device Management *Funds Put to Better Use - $10,034*	6

Reporting Requirements

Report Number	Date Issued	Title	Number of Open Recommendations
15-03	2/6/2015	Specially Protected Holdings	17
15-11	5/5/2015	Digitization Storage and Transfer Capabilities	1
15-13	8/24/2015	Human Resources Systems and Data Accuracy	3
15-14	9/29/2015	Space Management (Textual)	1
15-15	9/30/2015	Assessment of Cable Infrastructure	8
16-01	10/19/2015	Web Hosting Environment	20
16-02	1/16/2016	Compliance with FISMA, As Amended	7
16-05	3/25/2016	Publicly-Accessible Websites	12
16-07	5/17/2016	Refile Processes at Selected Federal Records Centers	5
17-AUD-01	10/28/2016	Enterprise-Wide Risk Assessment of NARA's Internal Controls	7
17-AUD-02	11/4/2016	Information System Inventory	6
17-AUD-03	11/4/2016	Compliance with the Federal Managers Financial Integrity Act for FY15	10
17-AUD-04	11/18/2016	Management Control over Microsoft Access Applications and Databases	4
17-AUD-06	11/15/2016	Procurement Program	19
17-AUD-07	2/19/2017	Compliance with Homeland Security Presidential Directive 12	3
17-AUD-08	3/15/2017	Adoption and Management of Cloud Computing	10
17-AUD-16	9/27/2017	FOIA Program	1
18-AUD-04	2/26/2018	Office of the Federal Register's Administration of the Electoral College Process	2
18-AUD-06	3/29/2018	Legacy Systems *Funds Put to Better Use - $45,350,000*	13

Reporting Requirements

Report Number	Date Issued	Title	Number of Open Recommendations
18-AUD-09	6/4/2018	Human Capital Practices	4
18-AUD-14	8/20/2018	Continuity of Operations (COOP) Readiness	10
19-AUD-01	11/15/2018	FY 2018 Consolidated Financial Statements	8
19-AUD-02	12/21/2018	Oversight of FY 2018 FISMA Assessment	21
19-AUD-03	12/20/2018	Presidential Libraries' Analog Processing	6
19-AUD-07	3/29/2019	Purchase Card Program *Funds Put to Better Use - $131,816*	9
19-AUD-10	6/11/2019	Oversight of Electronic Records Management in the Federal Government	9
20-AUD-02	11/8/2019	Compliance with Digital Accountability and Transparency Act of 2014	1
20-AUD-03	12/12/2019	Classified Information Systems	11
20-AUD-06	3/4/2020	Oversight and Management of Information Technology Contracts	7