



NATIONAL
ARCHIVES

OFFICE *of* INSPECTOR GENERAL

Fiscal Year 2022 Work Plan

November 8, 2021



Table of Contents

MESSAGE FROM THE INSPECTOR GENERAL 3

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION 4

OIG MISSION AND AUTHORITY 4

FY 2022 MANAGEMENT AND PERFORMANCE CHALLENGES 5

AUDITS AND EVALUATIONS FY 2022 6

 CARRY OVER AUDITS 6

 Mandatory 6

 Discretionary 7

 NEW AUDITS AND EVALUATIONS 10

 Mandatory 10

 Discretionary 11

INVESTIGATIONS – PRIORITIES, OBJECTIVES, AND INITIATIVES FOR FY 2022 13

Message from the Inspector General

I am pleased to present the National Archives and Records Administration (NARA) Office of Inspector General (OIG) fiscal year (FY) 2022 annual work plan. The plan provides our approach for conducting oversight work designed to help improve the economy, efficiency, and effectiveness of NARA's programs and operations, while also preventing and detecting fraud, waste, and abuse. We coordinated with NARA and other stakeholders to gain insight on work that will further ensure accountability and integrity in agency programs and operations.

The audit and evaluation work in the plan shows our carry over work from fiscal year 2021, as well as mandatory and discretionary work for fiscal year 2022. Our statutory mandates are our highest priority, and with our remaining resources, we focus on work areas that present the highest risks to the agency. As we move forward, we may need to adjust the plan to ensure we are focusing our attention on the highest risks facing NARA or respond to requests from Congress or other stakeholders. This may result in planned work being postponed or cancelled to meet those emerging needs. The investigations priorities provide insight on areas that we are paying attention to ensure integrity in NARA programs and operations.

As the nation's record keeper, NARA has an important mission in our democracy by providing public access to high-value government records. The OIG is charged with providing effective oversight to help NARA succeed in their mission. This is an agency that can affect the lives of each of our nation's citizens, and I look forward to the opportunities that lie ahead.



Dr. Brett M. Baker
Inspector General

National Archives and Records Administration

NARA drives openness through access to records. While NARA is currently updating their Strategic Plan, NARA's mission is stated: Our mission is to provide public access to Federal Government records in our custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

In FY 2021, NARA was appropriated \$377 million for operating expenses, including \$9.2 million to enhance the government's ability to electronically preserve, manage, and store government records, and up to \$2 million to implement the Civil Rights Cold Case Records Collection Act of 2018; \$9.5 million for repairs and restoration of archives facilities, \$6.5 million for the NHPRC, and \$4.8 million for Inspector General (IG) operations. NARA was subsequently provided with an extra \$50 million in emergency funds to address problems caused by the coronavirus pandemic at Federal Records Centers, and to accelerate processing of requests for military service records received during the pandemic. With approximately 2,583 employees, NARA operates 44 facilities nationwide.

OIG Mission and Authority

NARA's OIG was formally established in April 1989. The Inspector General Act, as amended (IG Act) contained in Public Law 100-504 states the IG is responsible for conducting and supervising independent audits and investigations of agency programs and operations; promoting economy, effectiveness, and efficiency within the agency; detecting and preventing fraud, waste, mismanagement, and abuse of agency programs and operations; Making recommendations designed to promote the economy, efficiency, and effectiveness of the agency. Unique in the Federal system, the IG is required to keep both the Archivist and Congress fully and currently informed about fraud and other serious problems, abuses, and deficiencies relating to NARA's programs and operations.

FY 2022 Management and Performance Challenges

In executing its mission, the IG summarizes what he considers to be the most significant management and performance challenges facing the NARA and assesses the agency's progress in addressing those challenges. The following summarizes those challenges based on legislative mandates, our experience, stakeholder input, and observations from our oversight work.

1. Records Request Backlog at the National Personnel Records Center (NPRC)
2. Information Technology (IT) Security
3. Office of Management and Budget (OMB) Memorandum M-19-21, Transition to Electronic Records
4. Expanding Public Access to Records
5. Electronic Records Archives (ERA)
6. Pandemic Response

Audits and Evaluations FY 2022

Carry Over Audits

Mandatory

Audit of NARA's Compliance with the Federal Information Security Modernization Act (FISMA) for FY 2021

The *FISMA of 2014* requires Federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source. FISMA also requires Agency IGs to assess the effectiveness of Agency information security programs and practices. IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. IGs are to consider both their and management's assessment of the unique missions, resources, and challenges when assessing the maturity of information security programs.

The objective of this audit is to evaluate the effectiveness of NARA's information security program and practices. Specifically, we will assess NARA's information security program in accordance with FISMA of 2014 and the Department of Homeland Security's FY 2021 Inspector General FISMA Reporting Metrics.

Audit of NARA's FY 2021 Financial Statements

In accordance with in accordance with the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 19-03), the OIG is required to audit the NARA's financial statements.

The objective of this audit is to express an opinion on whether NARA's financial statements are fairly presented, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Audit of NARA's Compliance Digital Accountability and Transparency (DATA) Act

The DATA Act, in part, requires Federal agencies to report financial and award data in accordance with the established Government-wide financial data standards. In May 2015, the OMB and Treasury published 57 data definition standards (commonly referred to as data elements) and required Federal agencies to report financial and award data in accordance with these standards for DATA Act reporting, in January 2017. Subsequently, and in accordance with the DATA Act, Treasury began displaying Federal agencies' data on USASpending.gov for taxpayers and policy makers in May 2017.

The DATA Act also requires the IG of each Federal agency to audit a statistically valid sample of the spending data submitted by its Federal agency and to submit to Congress a publicly available

report assessing the completeness, accuracy, timeliness, and quality of the data sampled; and the implementation and use of the Government-wide financial data standards by the Federal agency.

The objective of this audit is to assess the (1) completeness, timeliness, quality, and accuracy of financial and award data NARA submitted for publication on USASpending.gov, and (2) the implementation and use of the Government-wide financial data standards established by the OMB and the U.S. Department of the Treasury.

Discretionary

Audit of NARA's Holdings Protection Program

In 2009, NARA established the Holdings Protection Program and Team to serve as a nationwide resource for developing and administering policies to enhance holdings protection, reduce the loss of, and aid in the recovery of holdings. The team provides assistance and advice to agency offices and ensures holdings protection policies and procedures are being followed. In addressing how the agency safeguarded its holdings, the team also develops procedures, which increases holdings security, monitoring, and screening at NARA facilities nationwide. However, internal control weaknesses in holdings security date back to FY 2001 when NARA declared this area a FMFIA Material Weakness (downgraded in 2014 to a reportable condition). Given NARA's strategic goal of *make access happen*, risks in protecting records from theft and vandalism remain to some degree.

The objective of this audit is to determine whether NARA has controls in place to reasonably secure and protect holdings from theft or vandalism.

Audit of NARA's Processing of Discrimination Complaints

An Equal Employment Opportunity Complaint is an allegation of discrimination because of race, color, religion, national origin, sex (including sexual harassment and sexual orientation), and age, physical or mental handicap. The complaint may arise from a specific personnel action, such as employment, promotion, work assignment, selection for training, disciplinary action, or separation, or it may relate to prevailing conditions in an organization. NARA is responsible for implementing the discrimination complaint program required by *Title 29 of the Code of Federal Regulations, Part 1614, titled, Federal Sector Equal Employment Opportunity*, which mandates specific time frames for federal agencies to process, investigate, and issue agency decisions on discrimination complaints. These regulations are included in the Equal Employment Opportunity Commission policies, procedures, and guidance published in the *Management Directive 110 (MD-110)*.

The objective of this audit is to determine whether NARA processed discrimination complaints in a timely and efficient manner.

Audit of NARA's Off-boarding Process for Separating Employees, Contractors, and Volunteers

NARA in accordance with Federal law and regulation must ensure that all personnel ending their work or volunteer relationship with NARA, or relocating to a different office or facility account for any outstanding financial responsibilities. NARA must also ensure that the personnel return accountable items for which they are responsible, clear duties, and terminate access to IT systems.

The Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, establishes the requirement for each Government agency to issue Personal Identity Verification (PIV) compliant credentials, also referred to as PIV cards, to its Federal and contractor employees. In response, the U.S. General Services Administration offered USAccess as an efficient way for Federal agencies to issue PIV cards to their employees and contractors. PIV cards can be used to gain access to Federal facilities and information systems within an agency. In an effort to comply with the HSPD-12 requirement, NARA uses the PIV card to access buildings and some systems.

The objective of this audit is to assess the effectiveness of controls over the off-boarding process for separating employees, contractors, and volunteers.

Audit of NARA's Corporate Records Management Program

OMB in conjunction with NARA, issued Memorandum M-19-21, *Transition to Electronic Records* which focuses on records management, and directs Federal agencies to transition recordkeeping to a fully electronic environment that complies with all records management laws and regulations. The memorandum directs all Federal agencies to: (1) ensure that all Federal records are created, retained, and managed in electronic formats, with appropriate metadata; and (2) consistent with records management laws and regulations, develop plans to close agency-operated storage facilities for paper and other, analog records, and transfer those records to Federal Records Centers operated by NARA or commercial storage facilities. Also, the memorandum consolidates requirements from prior OMB records management guidance to ensure consistent, government-wide policy and practices and rescinds OMB M-12-18, *Managing Government Records Directive*, and OMB M-14-16, *Guidance on Managing Email*. Section I of M-19-21 establishes deadlines for all agencies to adopt electronic recordkeeping requirements, in a manner compliant with the Federal Records Act. Title 44 United States Code (U.S.C.) Chapter 31 and 44 U.S.C. Chapter 33 identifies responsibilities for the head of each Federal agency for records management.

The objective of this audit is to determine if NARA's internal records management program is effective and complies with all records management policies and procedures and serves as a model records management program.

Audit of NARA's Software Asset Management Process

Software licenses are agreements between suppliers and customers about the guidelines for use and distribution of software. Effective software license management allows organizations to maintain accurate software inventories to improve accountability, security, and compliance. OMB Memorandum 16-12, *Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing* addresses challenges agencies have in software licensing including but not limited to the purchasing and management of software licenses as well as accuracy of software inventories. The Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016 requires each Federal executive agency identified in FITARA, to develop a comprehensive software licensing policy that includes identifying clear roles and responsibilities and central oversight authority within the Federal executive agency for managing software licenses.

The objective of this audit is to determine if governance structures are in place to provide adequate direction and establish accountability for procuring, tracking, and monitoring software assets, in order to minimize shortage, waste, and security risks.

New Audits and Evaluations

Mandatory

Audit of NARA's Compliance with the FISMA for FY 2022

The *FISMA of 2014* requires Federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source. FISMA also requires Agency IGs to assess the effectiveness of Agency information security programs and practices. IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. IGs are to consider both their and management's assessment of the unique missions, resources, and challenges when assessing the maturity of information security programs.

The objective of this audit is to evaluate the effectiveness of NARA's information security program and practices. Specifically, we will assess NARA's information security program in accordance with FISMA of 2014 and the Department of Homeland Security's FY 2022 IG FISMA Reporting Metrics.

Audit of NARA's FY 2022 Compliance with the Payment Integrity Information Act (PIIA) of 2019

The *Improper Payments Elimination and Recovery Act of 2010* (IPERA) amended the *Improper Payments Information Act of 2002* and required agencies to identify and review all programs and activities they administer that may be susceptible to significant improper payments based on guidance provided by the OMB. On March 2, 2020, the *Payment Integrity Information Act of 2019* (PIIA) repealed IPERA (and other laws) but set forth similar improper payment reporting requirements, including an annual compliance report by Inspectors General.

Significant improper payments are defined as gross annual improper payments (i.e., the total amount of overpayments and underpayments) in the program exceeding (1) both 1.5 percent of program outlays and \$10,000,000 of all program or activity payments made during the fiscal year reported or (2) \$100,000,000 (regardless of all the improper payment percentage of total program outlays).

The objective of this audit is to determine whether NARA has met all requirements of the (PIIA) of 2019 in the Payment Integrity section of the FY 2021 Agency Financial Report/Performance and Accountability Report and accompanying materials. In addition, we will evaluate NARA's efforts to prevent and reduce improper payments.

Audit of NARA's FY 2022 Financial Statements

In accordance with in accordance with the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 19-03), the OIG is required to audit the NARA's financial statements.

The objective of this audit is to express an opinion on whether NARA's financial statements are fairly presented, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Discretionary

Evaluation of Records Request Backlog at the National Personnel Records Center (NPRC)

The National Personal Records Center (NPRC) is the central repository of personnel-related records for both military and civilian services. The NPRC stores records of individual military service pertaining to former service members who no longer have a service obligation. The Official Military Personnel File (OMPF) is a permanent record of the United States and becomes official property of NARA 62 years after the service member's separation from the military.

NPRC stores over 4 million cubic feet of military and civilian personnel, medical and related records in textual and micrographic formats in two separate facilities in the St. Louis metropolitan area. Due to the COVID-19 pandemic and the subsequent closure of NARA facilities across the nation, significant backlogs have accumulated in each of the customer-facing program offices, despite efforts to respond to requests remotely. The backlog at the NPRC has grown from 56,000 to 586,000 since March, 2020.

The objective of this evaluation is to evaluate the backlog of records requests by veterans and their families at the NPRC and make recommendations that will help efficiently reduce the backlog and improve the process moving forward.

Audit of NARA's Cloud Computing Services

In 2011, the Office of Management and Budget issued its Federal Cloud Computing Strategy which required agencies to use cloud infrastructure, as they planned new missions, supported applications, or consolidated existing applications. In 2019, the Federal Cloud Computing Strategy was updated, tasking Federal agencies to accelerate migration to cloud-based computing solutions and modernize information technology (IT) infrastructure. The strategy focused on enhancing security and high-quality IT service to the American people. In May 2021, the President issued an Executive order detailing his administration's goal to modernize Federal Government cybersecurity. Specifically, to keep pace with today's dynamic and increasingly sophisticated environment, the Federal government should accelerate the movement to secure cloud services, adopt security best practices, and develop migration plans for Zero Trust Architecture.

The objective of this audit is to reassess NARA's cloud computing efforts and examine whether the agency has effectively implemented plans, procedures, and controls to meet Federal and agency IT security requirements for protecting the confidentiality, integrity, and availability of data stored in the cloud.

Audit of NARA's Electronic Records Archives (ERA)

Electronic records are the future of government archiving, and NARA must become a world leader in preserving, storing, and presenting electronic records to meet its mission. NARA's plan to address this is the ERA system. ERA has become a "system of systems", and the original ERA Base System was not capable of meeting the nation's needs. Thus NARA is developing ERA 2.0. Some components of ERA 2.0 have been put into production and are used by some NARA staff who work with digital materials.

The objective of this audit is to evaluate NARA's progress in implementing ERA 2.0 in order to accept, store, and process records. With the implementation of OMB M-19-21, the vast volumes of electronic records that will need to be preserved are significant. NARA will need to ensure its processes for accepting, storing, and processing historically significant electronic records are sufficient to make them available to the public.

Evaluation of NARA's Response to the Coronavirus Pandemic

On January 31, 2020, the U.S. Department of Health and Human Services declared a public health emergency for the United States to aid the nation's healthcare community in responding to the Coronavirus Disease 2019 (COVID-19). On March 11, 2020, the COVID-19 outbreak was characterized as a pandemic by the World Health Organization. State and local jurisdictions rapidly enacted social distancing guidelines recommended by the Centers for Disease Control, and NARA took steps to protect their employees and mitigate the spread of a novel disease in their communities.

The objective of this evaluation is to evaluate the effects of the pandemic on NARA's workforce and operations.

Investigations Priorities, Objectives, and Initiatives for FY 2022

The OIG's Office of Investigations (OI) adds value to the agency's programs and operations by identifying and investigating allegations of fraud, waste, abuse, and misconduct leading to criminal, civil, administrative, and other remedies. Investigations typically originate as a result of a complaint to our Hotline program. Investigations, referrals, and inquiries emerge based on varying OIG criteria. The OIG's investigative program also established initiatives designed to monitor high-risk areas within NARA's programs and operations in order to identify vulnerabilities.

The following activities are planned for FY 2022 in the OI:

- Investigate Misconduct and Fraud Associated with NARA Programs and Operations

In FY 2022, the OI will continue to identify, investigate, and report instances of misconduct by NARA employees. Additionally, the OI will remain focused on identifying and combating fraud associated with NARA programs and operations to include the Stolen Valor and Military Records Fraud initiative involving records improperly obtained from the National Personnel Records Center. We also remain committed to identifying and recovering missing and stolen artifacts and records that are historically significant.

- Hotline Program

The OI operates a nationwide hotline program allowing individuals to report any suspicious activities or complaints through our website, by telephone, by email, or to a designated physical mailing address. All intakes are reviewed, and when warranted, we will do additional investigative work or refer the intake to the appropriate corresponding entity to address the issue.

- OIG National Outreach Program

The OI will continue to raise OIG awareness by reaching out to both internal NARA employees and external stakeholders and provide information on the OIG's mission, roles, and responsibilities. The OI will also continue to administer content on the OIG's public website and remain active in various professional working groups within the law enforcement and OIG community.

- Internal Reviews of OI Policy, Procedures, Accountable Property, and Annual Training

The OI will conduct an extensive review of its internal Special Agent Handbook and policies, and revise and update areas of concern based upon relevant legal updates or issues identified by our internal reviews to maintain compliance with the latest professional standards. The OI review team will also conduct reviews of accountable property, evidence, and other material to ensure compliance and identify any areas of vulnerability.

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 www.archives.gov/oig/ for more information, or contact us:

By telephone

Washington, DC, Metro area: 301- 837-3500

Toll-free: 800-786-2551

By mail

NARA OIG Hotline

P.O. Box 1821

Hyattsville, MD 20788-0821

By email

oig.hotline@nara.gov

By facsimile

301-837-3197

By online referral form

www.archives.gov/oig/referral-form/index.html

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.