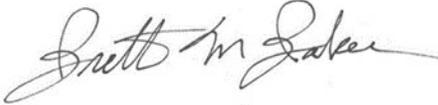




Inspector General

November 14, 2024

TO: Dr. Colleen Shogan
Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General 

SUBJECT: *Audit of NARA's Fiscal Year 2024 Consolidated Financial Statements*
OIG Report No. 25-AUD-01

The Office of Inspector General (OIG) contracted with Sikich to conduct an independent audit on the financial statements of the National Archives and Records Administration (NARA) as of and for the fiscal year ended September 30, 2024. The report should be read in conjunction with NARA's financial statements and notes to fully understand the context of the information contained therein.

Sikich is responsible for the attached auditors report dated November 13, 2024 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of Sikich. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with Generally Accepted Government Auditing Standards.

Results of the Independent Audit

Sikich issued an unmodified opinion on NARA's fiscal year 2024 financial statements. Sikich found:

- NARA's financial statements as of and for the fiscal year ended September 30, 2024, are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- No material weaknesses in internal control over financial reporting based on the limited procedures performed;
- One significant deficiency in internal control over financial reporting as of September 30, 2024; and
- No reportable noncompliance for fiscal year 2024 with provisions of applicable laws, regulations, contracts, and grant agreements tested.

The report contains ten repeated and three new recommendations to improve NARA's internal controls over financial reporting related to longstanding control deficiency in information technology controls. Management concurred with all of the recommendations. Based on your November 12, 2024 response to the formal draft report, we consider all the recommendations open.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this letter. As with all OIG products, we determine what information is publicly posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended*, we will provide copies of our report to congressional committees with oversight responsibility over NARA.

We appreciate the cooperation and assistance NARA extended to Sikich and my staff during the audit. Please contact me with any questions.

Attachment

cc: Merrily Harris, Executive Secretariat
William Bosanko, Deputy Archivist
Gary M. Stern, General Counsel
Jay Trainer, Acting Chief Operating Officer
Meghan Guthorn, Deputy Chief Operating Officer
Colleen Murphy, Acting Chief of Management and Administration, Chief Financial Officer, and Senior Accountable Official
Sheena Burrell, Chief Information Officer
Nicole Willis, Deputy Chief Information Officer
Kimm Richards, Accountability
Carol Seubert, Senior Auditor
Teresa Rogers, Senior Program Auditor
Eric Good, Senior Program Auditor
United States Senate Homeland Security and Governmental Affairs Committee
United States House of Representatives Committee on Oversight and Reform



333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

INDEPENDENT AUDITORS' REPORT

Inspector General
National Archives and Records Administration

Archivist of the United States
National Archives and Records Administration

In our audit of the fiscal year 2024 financial statements of the National Archives and Records Administration (NARA), we found:

- The financial statements as of and for the fiscal year ended September 30, 2024, are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- No material weaknesses in internal control over financial reporting based on the limited procedures we performed;
- One significant deficiency in internal control over financial reporting as of September 30, 2024; and
- No reportable noncompliance for fiscal year 2024 with provisions of applicable laws, regulations, contracts, and grant agreements that we tested.

The following sections contain:

1. Our report on NARA's financial statements, including an other-matter paragraph related to the prior-period financial statements having been audited by a predecessor auditor, required supplementary information (RSI), and other information included with the financial statements; and
2. Other reporting required by *Government Auditing Standards*, which is our report on NARA's (a) internal control over financial reporting and (b) compliance and other matters. This section also includes a summary of NARA's comments on our report.

REPORT ON THE AUDIT OF THE FINANCIAL STATEMENTS

Opinion

We have audited the consolidated financial statements of NARA, which comprise the consolidated balance sheet as of September 30, 2024, and the related consolidated statement of net cost, consolidated statement of changes in net position, and combined statement of budgetary resources for the fiscal year then ended, and the related notes to the financial statements (collectively, the basic financial statements).

In our opinion, the accompanying financial statements present fairly, in all material respects, the financial position of NARA as of September 30, 2024, and its net cost of operations, changes in net position, and budgetary resources for the fiscal year then ended, in accordance with accounting principles generally accepted in the United States of America.

Basis for Opinion

We conducted our audit in accordance with auditing standards generally accepted in the United States of America (GAAS); standards applicable to financial statement audits contained in Generally Accepted Government Auditing Standards (GAGAS), issued by the Comptroller General of the United States; and guidance contained in Office of Management and Budget (OMB) Bulletin 24-02, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards and OMB Bulletin 24-02 are further described in the Auditors' Responsibilities for the Audit of the Financial Statements subsection of our report. We are required to be independent of NARA and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audit. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Other Matters

NARA's financial statements as of and for the year ended September 30, 2023, were audited by CliftonLarsonAllen, whose Independent Auditors' Report thereon dated November 13, 2023, expressed an unmodified opinion on those financial statements. On January 1, 2024, we acquired the federal practice of CliftonLarsonAllen. We were not engaged to audit, review, or apply any procedures to NARA's fiscal year 2023 financial statements and, accordingly, we do not express an opinion or any other form of assurance on the fiscal year 2023 financial statements.

Responsibilities of Management for the Financial Statements

Management is responsible for (1) the preparation and fair presentation of the financial statements in accordance with U.S. generally accepted accounting principles; (2) the preparation, measurement, and presentation of the RSI in accordance with U.S. generally accepted accounting principles; (3) the preparation and presentation of other information included in NARA's Agency Financial Report, and ensuring the consistency of that information with the audited financial statements and the RSI; and (4) the design, implementation, and maintenance of effective internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditors' report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS, GAGAS, and OMB guidance will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements, including omissions, are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgments made by a reasonable user based on the financial statements.

In performing an audit in accordance with GAAS, GAGAS, and OMB guidance, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements in order to obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control over financial reporting. Accordingly, no such opinion is expressed.



- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements.
- Perform other procedures we consider necessary in the circumstances.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the audit.

Required Supplementary Information

Accounting principles generally accepted in the United States of America and OMB Circular No. A-136, *Financial Reporting Requirements*, require that the Management's Discussion and Analysis (MD&A) and other RSI be presented to supplement the basic financial statements. Such RSI is the responsibility of management and, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board (FASAB) and OMB, who consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, and historical context. We have applied certain limited procedures to the RSI in accordance with auditing standards generally accepted in the United States of America. These procedures consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We did not audit, and we do not express an opinion or provide any assurance on the information because the limited procedures we applied do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

NARA's other information contains a wide range of information, some of which is not directly related to the financial statements. This information is presented for purposes of additional analysis and is not a required part of the financial statements or the RSI. Management is responsible for the other information included in NARA's Agency Financial Report. The other information comprises the *Summary of Financial Statement Audit and Management Assurances*, *OIG Report on Top Management Challenges Facing NARA*, *Payment Integrity Information Act Reporting*, and *Fraud Reduction Report* but does not include the financial statements and our auditor's report thereon. Our opinion on the financial statements does not cover the other information, and we do not express an opinion or any form of assurance thereon.

In connection with our audit of the financial statements, our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the financial statements, or the other information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the other information exists, we are required to describe it in our report.

OTHER REPORTING REQUIRED BY GOVERNMENT AUDITING STANDARDS

Report on Internal Control over Financial Reporting and on Compliance and Other Matters

Internal Control over Financial Reporting

In connection with our audit of NARA's financial statements, we considered NARA's internal control over financial reporting, consistent with our auditors' responsibilities discussed below.

Results of Our Consideration of Internal Control over Financial Reporting

Our consideration of internal control over financial reporting was for the limited purpose described below, and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies or to express an opinion on the effectiveness of NARA's internal control over financial reporting. Given these limitations, during our audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, material



weaknesses may exist that have not been identified. We identified certain deficiencies in internal control over financial reporting that we consider to be a significant deficiency, described below and in Appendix A.

Longstanding Control Deficiency in Information Technology (IT) Controls

NARA did not substantially address previously identified deficiencies in its IT general control categories of access controls, configuration management, and incident response. These unresolved control deficiencies impact the effectiveness of NARA's IT security program and internal controls over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

During our fiscal year 2024 audit, we identified deficiencies in NARA's internal control over financial reporting that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant NARA management's attention. We have communicated these matters to NARA management and, where appropriate, will report on them separately.

Basis for Results of Our Consideration of Internal Control over Financial Reporting

We performed our procedures related to NARA's internal control over financial reporting in accordance with GAGAS.

Responsibilities of Management for Internal Control over Financial Reporting

NARA management is responsible for designing, implementing, and maintaining effective internal control over financial reporting relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibilities for Internal Control over Financial Reporting

In planning and performing our audit of NARA's financial statements as of and for the fiscal year ended September 30, 2024, in accordance with GAGAS, we considered NARA's internal control relevant to the financial statement audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control over financial reporting. Accordingly, we do not express an opinion on NARA's internal control over financial reporting. We are required to report all deficiencies that are considered to be significant deficiencies or material weaknesses. We did not consider all internal controls relevant to operating objectives, such as those controls relevant to preparing performance information and ensuring efficient operations.

Definition and Inherent Limitations of Internal Control over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements due to fraud or error.



Intended Purpose of Report on Internal Control over Financial Reporting

The purpose of this report is solely to describe the scope of our consideration of NARA's internal control over financial reporting and the results of our procedures, and not to provide an opinion on the effectiveness of NARA's internal control over financial reporting. This report is an integral part of an audit performed in accordance with GAGAS in considering internal control over financial reporting. Accordingly, this report on internal control over financial reporting is not suitable for any other purpose.

Compliance and Other Matters

In connection with our audit of NARA's financial statements, we tested compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements consistent with our auditors' responsibilities discussed below.

Results of Our Tests for Compliance with Laws, Regulations, Contracts, and Grant Agreements

Our tests for compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements disclosed no instances of noncompliance or other matters for fiscal year 2024 that would be reportable under GAGAS. However, the objective of our tests was not to provide an opinion on compliance with laws, regulations, contracts, and grant agreements applicable to NARA. Accordingly, we do not express such an opinion.

Basis for Results of Our Tests for Compliance with Laws, Regulations, Contracts, and Grant Agreements

We performed our tests of compliance in accordance with GAGAS. Our responsibilities under those standards are further described in the Auditor's Responsibilities for Tests of Compliance subsection below.

Responsibilities of Management for Compliance with Laws, Regulations, Contracts, and Grant Agreements

NARA management is responsible for complying with laws, regulations, contracts, and grant agreements applicable to NARA.

Auditors' Responsibilities for Tests of Compliance with Laws, Regulations, Contracts, and Grant Agreements

Our responsibility is to test compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements that have a direct effect on the determination of material amounts and disclosures in NARA's financial statements, and to perform certain other limited procedures. Accordingly, we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to NARA. We caution that noncompliance may occur and not be detected by these tests.

Intended Purpose of Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements

The purpose of this report is solely to describe the scope of our testing of compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, and the results of that testing, and not to provide an opinion on compliance. This report is an integral part of an audit performed in accordance with GAGAS in considering compliance. Accordingly, this report on compliance with laws, regulations, contracts, and grant agreements is not suitable for any other purpose.

NARA's Comments

NARA's comments on this report are included in Appendix B. NARA concurred with the findings in our report.

Sikich CPA LLC

Alexandria, VA
November 13, 2024



APPENDIX A Significant Deficiency

Longstanding Control Deficiency in Information Technology Controls (Modified Repeat Finding)

NARA relies extensively on information technology (IT) systems to accomplish its mission and to prepare its financial statements. Internal controls over these financial and supporting operations are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts. NARA staff use IT system controls to initiate and authorize financial transactions at user workstations, which transmit those transactions across the network to servers that record, process, summarize, and report financial transactions in support of the financial statements.

NARA did not substantially address previously identified deficiencies in its IT general control categories of access controls, configuration management, and incident response. These unresolved control deficiencies impact the effectiveness of NARA's IT security program and internal controls over financial reporting. Below, we have summarized our key findings by general control category:

Access Controls – We identified weaknesses related to privileged user access permissions and weak password configurations. This occurred because NARA is not reviewing service account passwords to determine if each service account used a unique password. Furthermore, NARA is not reviewing domain user accounts to determine if weak passwords were being used. This increases the risk of compromise by an attacker to upload malware, steal sensitive data, add or delete users, change system configurations, and alter logs to conceal his or her actions.

In addition, we found prior year weaknesses related to timely disabling of user accounts, multi factor user authentication, and identity and access management policy or strategy, remained unresolved. These weaknesses occurred because NARA is still a) developing an electronic form with automated checks and notifications to ensure new hire training is completed within the initial time frame given to new users, with user accounts disabled if not completed, b) implementing a process requiring multifactor authentication using personal identity verification for all privileged users, servers and applications, and c) further refining a draft identity and access management implementation plan. Additional access controls should be established to ensure user accounts are more effectively managed.

Configuration Management – We noted that NARA has not resolved prior year weaknesses related to the detection, remediation, and monitoring of high and critical risk vulnerabilities for software patches and updates, nor has it resolved system configuration weaknesses on NARA systems that have been publicly known since 2023 or earlier. In addition, we found prior year unresolved weaknesses related to migration of applications to vendor supported operating systems. These IT control deficiencies occurred as a result of an ineffective patch and vulnerability management program, as well as inadequate oversight by NARA management. Absent an effectively implemented and enforced configuration management program that addresses significant security weaknesses, there is an increased risk that individuals may inadvertently or deliberately disclose, manipulate, or misappropriate financial information.

Incident Response – NARA's implementation and maturity of event log management did not meet logging requirements in accordance with Office of Management and Budget (OMB) Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. NARA management indicated they are making progress to leverage service offerings from the Department of Justice for a Security Information and Event Management (SIEM) logging solution to capture security related log events to move NARA towards meeting the requirements. Therefore, NARA indicated it is in the process of trying to acquire funding to continue this service and expand its SIEM solution to consume more logs moving forward.

Cyberattacks underscore the importance of increased government visibility, before, during and after a cybersecurity incident. Information from logs on Federal information systems (for both on-premises

APPENDIX A Significant Deficiency

systems and connections hosted by third parties) is invaluable in detecting, investigating, and remediating cyber threats. By not achieving the required maturity levels, NARA is not meeting logging requirements of the highest criticality. Event logging capabilities are therefore not effective.

We based our testing on the following key criteria:

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (includes updates as of December 10, 2020):

- AC-6 Least Privilege, Privileged Accounts - Control Enhancement 5:
Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
- IA-5 Authenticator Management, Password Based Authentication- Control Enhancement 1:
 - a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
 - b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
- SI-2 Flaw Remediation
 - a. Identify, report, and correct system flaws;
 - b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
 - c. Install security-relevant software and firmware updates within [Assignment: organization – defined time period] of the release of the updates; and
 - d. Incorporate flaw remediation into the organizational configuration management process.
- SA-22 Unsupported System Components
 - a. Replaces system components when support for the components is no longer available from the developer, vendor, or manufacturer;
- CM-6 Configuration Settings
 - a. Establish, document configuration settings for components employed within the system that reflects the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
 - b. Implement the configuration settings;
 - c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
 - d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

OMB Memorandum A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*:

- Establishes minimum requirements for Federal Information Programs and assigned federal agency responsibilities for the security of information and information systems. The Circular specifically prohibits agencies from the use of unsupported information systems and system components and requires agencies to ensure that systems and components that cannot be appropriately protected or secured are given high priority for upgrade or replacement. In

APPENDIX A Significant Deficiency

addition, the Circular requires agencies to implement and maintain current updates and patches for all software and firmware components of information systems. Additionally, the Circular requires system security plans to be consistent with guidance issued by NIST.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, establishes:

A maturity model to guide the implementation of requirements across event log tiers designed to help agencies prioritize their efforts and resources to achieve full compliance with requirements for implementation, log categories, and centralized access. OMB M-21-31 further requires that agencies forward all required event logs, in near real-time and on an automated basis, to centralized systems responsible for security information and event management.

The identified weaknesses could be potentially exploited, intentionally or unintentionally, to undermine the integrity and completeness of data processed by NARA's financial management systems, including its feeder systems.

Recommendations:

We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to the following ten repeat and three new recommendations:

1. Implement a process to ensure accounts with access to the Domain Administrators group are appropriately assigned based on job responsibilities. If determined that an account can be configured with more restrictive access, then implement a process to revoke the Domain Administrator group membership and apply the most restrictive access. (New Recommendation)
2. Develop and implement policies and procedures for network user accounts to:
 - a. Create unique passwords for each service account;
 - b. Maintain a list of commonly used, expected, or compromised passwords;
 - c. Update the list on an organization defined timeframe and when organizational passwords are suspected to have been compromised directly or indirectly;
 - d. Verify (such as through regular password audits or system configurations), when users create or update passwords, the passwords are not found on the list of commonly used, expected, or compromised passwords. (New Recommendation)
3. Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements. (Prior Recommendation)
4. Coordinate with other departments as necessary to implement an authoritative data source which provides the current status of NARA contractors and volunteers at the enterprise level. (Prior Recommendation)
5. Enforce mandatory Personal Identity Verification (PIV) card authentication for all NARANet users, in accordance with OMB requirements. (Prior Recommendation)
6. Continue and complete efforts to require PIV authentication for all privileged users, servers, and applications, through NARA's identity and access management project and other efforts. (Prior Recommendation)

APPENDIX A

Significant Deficiency

7. Ensure a comprehensive identity, credential, and access management (ICAM) policy or strategy, which includes the establishment of related standard operating procedures, identification of stakeholders, communicating relevant goals, task assignments, and measure and reporting progress is developed and implemented. (Prior Recommendation)
8. Document and implement a process to track and remediate persistent configuration vulnerabilities, or document acceptance of the associated risks. (Prior Recommendation)
9. Implement remediation efforts to address security deficiencies on affected systems identified, to include enhancing its patch and vulnerability management program as appropriate, or document acceptance of the associated risks. (Prior Recommendation)
10. Fully complete the migration of applications to vendor supported operating systems. (Prior Recommendation)
11. Ensure the Information System Security Officers are reviewing system configuration compliance scans monthly as required within NARA's *Configuration Compliance Standard Operating Procedure*. (Prior Recommendation)
12. Enhance current procedures to ensure that new NARA users who do not complete their initial security awareness training, have their accounts automatically disabled in accordance with timeframes promulgated within the Privacy and Awareness Handbook. (Prior Recommendation)
13. Implement requirements across all event logging maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31. (New Recommendation)

APPENDIX B NARA's Comments



Archivist of the
United States

Date: November 12, 2024
To: Dr. Brett M. Baker
Inspector General
From: Dr. Colleen J. Shogan
Archivist of the United States
Subject: Management Response to the FY2024 Financial Statement Audit

Thank you for the opportunity to review your *Independent Auditor's Report* on the financial statement audit of the National Archives and Records Administration for the fiscal year ending September 30, 2024.

I am pleased to have received an unmodified or "clean" independent audit opinion on our financial statements. An unmodified opinion recognizes NARA's commitment to producing accurate and reliable financial statements and supports our efforts to continuously improve our financial management program.

NARA acknowledges the Information Technology challenges identified in this report and concurs with the recommendations of the independent auditor. I appreciate the work performed by the auditor in this area and will ensure the auditor's findings and recommendations are incorporated into NARA's action plan.

I would like to thank the Office of Inspector General and Sikich CPA LLC for their cooperative and professional approach in the conduct of this audit.



DR. COLLEEN J. SHOGAN
Archivist of the United States



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, we also maintain an online referral form. Walk-ins are always welcome.

Visit www.naraoig.oversight.gov for more information, or contact us:

By telephone

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

Toll-free: 800-786-2551

By facsimile

301-837-3197

By online complaint form

<https://naraoig.oversight.gov/online-complaint-form>

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 <https://naraoig.oversight.gov/oig-contractor-reporting-form>.