



Inspector General

December 18, 2025

TO: Jim Byron
Senior Advisor to the Acting Archivist

FROM: William Brown
Acting Inspector General

SUBJECT: *Audit of NARA's Fiscal Year 2025 Financial Statements*
OIG Report No. 26-AUD-01

The Office of Inspector General (OIG) contracted with Sikich CPA LLC (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, 2025. 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 December 18, 2025, 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 2025 financial statements. Sikich found:

- NARA's financial statements as of and for the fiscal year ended September 30, 2025, 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 Sikich performed, although internal controls could be improved;
- Two significant deficiencies in internal control over financial reporting as of September 30, 2025; and
- No reportable noncompliance for fiscal year 2025 with provisions of applicable laws, regulations, contracts, and grant agreements that were tested.

The report contains eight new recommendations to improve NARA's internal controls over financial reporting. Management concurred with all of the recommendations. Based on your December 18, 2025 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



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

SIKICH.COM

INDEPENDENT AUDITORS' REPORT

Acting Inspector General
National Archives and Records Administration

Senior Advisor to the Acting Archivist of the United States
National Archives and Records Administration

In our audit of the fiscal year 2025 financial statements of the National Archives and Records Administration (NARA), we found:

- NARA's financial statements as of and for the fiscal year ended September 30, 2025, 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, although internal controls could be improved;
- Two significant deficiencies in internal control over financial reporting as of September 30, 2025; and
- No reportable noncompliance for fiscal year 2025 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 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 NARA's comments on our report.

REPORT ON THE AUDIT OF THE FINANCIAL STATEMENTS

Opinion

We have audited the financial statements of NARA, which comprise the balance sheet as of September 30, 2025, and the related statement of net cost, 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 financial statements).

In our opinion, the accompanying financial statements present fairly, in all material respects, NARA's financial position as of September 30, 2025, 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.

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 (1) obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and (2) 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 of the financial statements 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.
- 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 financial statement 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 financial statements. Such RSI is the responsibility of management and, although not a part of the 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 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: (1) inquiring of management about the methods of preparing the RSI; and (2) comparing the RSI for consistency with management's responses to our inquiries, the financial statements, and other knowledge we obtained during our audit of the financial statements, in order to report omissions or material departures from FASAB and OMB guidelines, if any, identified by these limited procedures. We did not audit and we do not express an opinion or provide any assurance on the RSI because the limited procedures we applied do not provide 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, Inspector General's Top Management Challenges, 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 2025 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, material weaknesses or significant deficiencies may exist that have not been identified.

A *deficiency in internal control over financial reporting* 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 2025 audit, we identified certain deficiencies in NARA's internal control over financial reporting that we consider to be significant deficiencies, as described in **Appendix A**.

During our fiscal year 2025 audit, we also 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 and OMB audit guidance.



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, 2025, 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 internal control over financial reporting are to provide reasonable assurance that:

- 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.
- 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 Reporting 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 and Other Matters

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 2025 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 and Other Matters

We performed our tests of compliance in accordance with GAGAS and OMB audit guidance.

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 laws, regulations, contracts, and grant agreements applicable to NARA 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 Reporting on Compliance and Other Matters

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 and other matters 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
December 18, 2025



APPENDIX A: SIGNIFICANT DEFICIENCIES

During our engagement to audit the fiscal year 2025 National Archives and Records Administration (NARA) financial statements, we identified deficiencies in internal control over financial reporting. These deficiencies include two significant deficiencies, as described in this appendix. NARA management was aware of these deficiencies and had already begun preparing and planning corrective actions. For brevity and clarity, we have not provided all the details related to specific programs, systems, or account balances in this appendix. We have provided those details separately to NARA management and other stakeholders through Notices of Findings and Recommendations.

SIGNIFICANT DEFICIENCY 1: INTERNAL CONTROL PROGRAM

1a. Risk Assessment

Condition

NARA did not document whether its prior risk assessment remained valid and appropriate in consideration of changes to its operating environment. Although a risk assessment was completed for FY 2024, there is no documentation to support that management reevaluated or updated the assessment in FY 2025.

Criteria

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states:

The management of risk must be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary... At a minimum, management's risk management review processes must ensure that all aspects of the risk management processes are reviewed at least once a year.¹

Similarly, the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (the "Green Book"), states:

...changing conditions often prompt new risks or changes to existing risks that need to be assessed.²

Consistent with these standards, NARA 161, Appendix B, states:

At the beginning of each fiscal year, program owners and functions owners review and revise as appropriate, the programs and functions of each office to form the basis against which internal controls will be assessed for the coming fiscal year.³

¹ OMB Circular A-123 (July 2016), *Management's Responsibility for Enterprise Risk Management and Internal Control*, Section II. *Establishing Enterprise Risk Management in Management Practices*, Sub-Section C. *Implementation*

² GAO's Green Book (May 2025), Section 9.13, *Identify, Analyze, and Respond to Risk Related to Significant Changes*

³ NARA 161, (Revised 2017) Appendix B, *Internal Control Program Cycle*, Section 1a. *Beginning of Fiscal Year*



Cause

NARA did not follow the requirements outlined in its Internal Control Program policy, NARA 161, which requires an annual risk assessment at the beginning of each fiscal year. In addition, in fiscal year 2025, NARA issued its Management Team Risk Assessment (MTRA) standard operating procedures (SOP) guidance, which states that risk assessments will be performed no more than once every 2 years, creating a discrepancy between the established ICP policy and the new assessment procedural guidance.

Under the MTRA SOP, NARA is not required to document an annual reassessment of its risk environment that reflects OMB Circular A-123's expectation for agencies to maintain a current and comprehensive risk assessment to support its annual risk profile submission. Additionally, the SOP lacks necessary provisions for conducting periodic risk assessments to evaluate the effectiveness of the current risk exposure actions.

NARA currently performs remediation efforts to correct these matters and enhance its internal control framework, including the creation of an SOP to formalize its risk assessment process and improvements to its OMB Circular A-123 testing methodology.

Effect

NARA cannot demonstrate that it performed a comprehensive reassessment of its risk environment in fiscal year 2025. Inadequate assessment increases the risk that the agency may fail to identify and timely respond to relevant financial reporting risks in an effective manner. Additionally, NARA's fiscal year 2025 risk profile may not accurately consider and reflect NARA's current risk environment.

1b. Complementary User Entity Controls

Condition

NARA did not test the implementation and operating effectiveness of the complementary user entity controls (CUECs) identified in the System and Organization Controls (SOC) 1 Type 2 reports of its service organizations. Although these reports outline specific CUECs necessary for the control effectiveness of the service organization, NARA has not performed procedures to verify whether applicable CUECs have been implemented and are functioning as intended within NARA's own control environment.

Criteria

OMB Circular A-123, states:

If the processes provided by the third party service organization is significant to an Agency's internal control objectives, then the Agency is responsible for establishing user Agency controls that complement the service organization's controls. Management still retains overall responsibility and accountability for all controls related to the processes provided by the third party, and must monitor the process as a whole to make sure it is effective.⁴

⁴ OMB Circular A-123 (July 2016), *Management's Responsibility for Enterprise Risk Management and Internal Control, Section III. Establishing and Operating an Effective System of Internal Control, sub-section B1. Service Organizations*



Similarly, GAO Green Book, states:

If controls a service organization performs are necessary to achieve the entity's control objectives, the entity implements any complementary user entity controls and other controls, as appropriate, related to the use of the service organizations.⁵

Consistent with these standards, NARA 161, Appendix C, states:

Management should design control activities to achieve objectives and respond to risks. It further states, *“Management should design the NARA’s information system and related control activities to achieve objectives and respond to risks.*⁶

Cause

NARA has not developed and implemented comprehensive procedures to assess SOC 1 Type 2 reports control activities and to evaluate the design and operating effectiveness of applicable CUECs relevant to NARA.

Effect

Without implementing and evaluating internal controls applicable to CUECs, NARA may be unable to place appropriate reliance on the controls of its service organizations. This increases the risk that control deficiencies in outsourced processes go undetected, potentially affecting the integrity of financial reporting and compliance with internal control requirements.

1c. Materiality Calculation

Condition

NARA did not calculate or document materiality thresholds as part of its assessment process of internal control over financial reporting. Specifically, NARA did not document how materiality consideration is applied in its assessment process, including its use in determining the scope and extent of internal control testing and in evaluating the significance of identified control deficiencies.

Criteria

OMB Circular A-123, Appendix A, states:

*Management has responsibility for determining the materiality of internal control activities and whether these materiality thresholds align with the level of control activities needed to provide reasonable assurances.*⁷

Cause

NARA management stated that it relied on the materiality thresholds included in the prior-year Management Representation Letter by its external auditors, but that it did not establish

⁵ GAO Green Book (May 2025), Section OV4.04, *External Parties*, Section OVA.04

⁶ NARA 161, (Revised 2017) Appendix C, *Internal Control - An Overview*, Control Activities

⁷ OMB Circular A-123 (June 2018), *Management’s Responsibility for Enterprise Risk Management and Internal Control*, Appendix A, Materiality



or document its own internal materiality thresholds for the purpose of internal control over financial reporting assessment.

Effect

Without materiality thresholds established independently by management, NARA is unable to demonstrate that it consistently and objectively assesses the internal control deficiencies and their impact. Additionally, it increases the risk of underreporting control issues, potentially leading to misinformed management decisions, inadequate corrective actions, and noncompliance with federal internal control requirements. Furthermore, it also limits transparency and comparability in financial reporting. This approach does not align with the expectations outlined in OMB Circular A-123, which requires agencies to define and use materiality to support risk-based scoping and evaluation of internal control deficiencies.

Recommendations

We recommend that NARA's Chief Financial Officer:

Risk Assessment

1. Revise NARA 161, *NARA's Internal Control Program*, to establish a process to periodically evaluate whether the prior-year risk assessment remains valid and appropriate to address significant organizational or operational changes.
2. Document through a written formal memorandum any periodic risk evaluations and the decision whether or not to update the last prior-year assessment to reflect the current risk environment. This memorandum should include a clear justification and documentation of the evaluation performed and be reviewed and approved by the Management Control Oversight Council to ensure appropriate oversight and accountability.

CUECs

3. Establish NARA policy for reviewing System and Organization Controls 1 Type 2 reports and evaluating complementary user entity controls. This policy related to control activities should be integrated into the agency's internal control over financial reporting framework and include:
 - a. Identification and Evaluation of CUECs
 - b. Assignment of Responsibility
 - c. Assessment of Control Effectiveness
 - d. Documentation and Oversight

Materiality Calculation

4. Establish a written formalized methodology for calculating materiality thresholds in accordance with Office of Management and Budget Circular A-123, Appendix A.



SIGNIFICANT DEFICIENCY 2: LONG-STANDING 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:

2a. Access Controls

We identified weaknesses related to privileged user access permissions and weak password configurations. This occurred because NARA does not review service account passwords to determine whether each service account used a unique password. Furthermore, NARA is not reviewing domain user accounts to determine whether 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/or alter logs to conceal their actions.

Additionally, NARA did not retain access request forms as evidence of access approval for a sample of users with access to NARANet. NARA indicated that the users were initially created prior to the existing ServiceNow system; as a result, they were unable to provide their access request forms. Without documentation of approved user access requests, there is an increased risk that users could be given access to sensitive or confidential data and systems that exceed their roles and responsibilities.

Additionally, 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. needs to identify and rectify issues related to the unintended re-enabling of accounts previously disabled due to inactivity;
- c. implementing a process requiring multi-factor authentication using personal identity verification for all privileged users, servers and applications; and
- d. further refining a draft identity and access management implementation plan.

If user accounts are not disabled in a timely manner when no longer needed, there is an increased risk unauthorized individuals may access these accounts. Additionally, the lack of



multifactor authentication means NARA information systems are more susceptible to attacks on user accounts.

2b. 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.

Additionally, 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. NARA management indicated they will develop a schedule or timeline for modernization or migration of systems based on the availability of funding.

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.

2c. Incident Response

We noted that NARA has not resolved prior-year weaknesses related to the implementation and maturity of event log management to meet logging requirements in accordance with OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. NARA management indicated that—although they are collecting many of the required logs and forwarding to the Security Information and Event Management system, as prescribed by OMB M-21-31—they are awaiting additional funding as their current licensing will not allow the further ingestion of logs from additional systems. As a result, NARA may not collect all meaningful and relevant data on suspicious events. This may, in turn, increase the risk that NARA inadvertently miss the potential scope of veracity of suspicious events or attacks.

Criteria

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*:

- *AC-2 Account Management*
 - ...
 - g. *Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;*
 - h. *Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];*
 - i. *Authorize access to the system based on:*
 1. *A valid access authorization;*
 2. *Intended system usage; and*

3. [Assignment: organization-defined attributes (as required)];
 - AC-6 Least Privilege, Control Enhancement 5: Privileged Accounts:
Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
 - IA-2 Identification and Authentication (Organizational Users), Control Enhancement 1: Multifactor Authentication to Privileged Accounts:
Implement multi-factor authentication for access to privileged accounts.
 - IA-2 Identification and Authentication (Organizational Users), Control Enhancement 2: Multifactor Authentication to Non-Privileged Accounts:
Implement multi-factor authentication for access to non-privileged accounts.

IA-5 Authenticator Management, Control Enhancement 1: Password-Based Authentication:

- 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);*

OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management*, stipulates:

Section IV. Shifting the Operating Model beyond the Perimeter

2. *Each agency shall define and maintain a single comprehensive Identity, Credential, and Access Management (ICAM) policy, process and technology solution roadmap, consistent with agency authorities and operational mission needs. These items should encompass the agency's entire enterprise, align with the Government-wide federal ICAM architecture and Continuous Diagnostics Management (CDM) requirements, incorporate applicable federal policies, standards, playbooks, and guidelines, and include roles and responsibilities for all users.*

The *NARA User Account and Privileged User Account Management Standard Operating Procedure (SOP)*, Version 8.0 (December 31, 2024), states:

All accounts will be disabled after 60 days and de-provisioned after 90 days.

Additionally, Section 5.27, *Account Deprovision Procedure*, states:

When a user separates or terminates from NARA and no longer needs access to NARANet, the account is disabled and scheduled for de-provisioning. If the account disablement decision changes, a ten business day window is provided.



When an account has been inactive for over 30 days, the OIG will receive an email notification with the user's name. After 60 days, the user will be disabled, and after 90 days, the user will be de-provisioned. If a user has been de-provisioned for over 180 days, they will be removed from the system.

The NARA System Security Plan for NARANet General Support System Common Controls states the following regarding with regard to security control Risk Assessment (RA-5):

Vulnerability Scanning, states, "(d), Remediates legitimate vulnerabilities within the NARA-defined timeframes for 30 days (Critical, High) and 60 days (Moderate, Low) in accordance with organizational assessment of risk."

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.

Effect

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 implement the prior-year open recommendations from the *Audit of NARA's Fiscal Year 2024 Consolidated Financial Statements* (OIG Report No. 25-AUD-01) and the below new recommendations:

5. Ensure access request forms are resubmitted for the NARANet accounts noted in the audit finding. (New Recommendation)
6. Implement procedures (e.g., patching, configuration weaknesses) to remediate security vulnerabilities identified by vulnerability scans within the defined remediation timeframes in the *NARANet General Support System Common Controls System Security Plan* and document an acceptance of associated risks as appropriate. (New Recommendation: OIG Report 25-AUD-08, Recommendation 2)
7. Conduct an assessment to: 1) identify applications running on unsupported platforms and their associated servers; 2) group applications and establish a migration schedule; and 3) migrate applications to vendor-supported platforms. For applications or operating systems that cannot be migrated, document the associated risks and obtain formal acceptance for continued operation. (New Recommendation: OIG Report 25-AUD-08, Recommendation 3)



8. Disable non-essential certificate service endpoints and web enrollment. Additionally, enable features that enhance the protection and handling of credentials when authenticating network connections. (New Recommendation: OIG Report 25-AUD-08, Recommendation 4)



APPENDIX B: MANAGEMENT'S RESPONSE

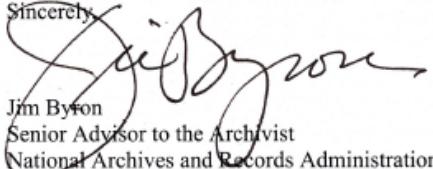
Date: December 18, 2025
To: William C. Brown, Acting Inspector General
From: Jim Byron, Senior Advisor to the Acting Archivist of the United States
Subject: Management Response to the FY2025 Financial Statement Audit

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, 2025.

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 Internal Control and 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.

Sincerely,

Jim Byron
Senior Advisor to the Archivist
National Archives and Records Administration



APPENDIX C: OIG HOTLINE CONTACT INFORMATION

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 accept emails through an online referral form.

Visit <https://naraoig.oversight.gov/> for more information, or contact us:

Contact the OIG Hotline

[Online Complaint Form | Office of Inspector General OIG](#)

Contact the OIG by telephone and FAX

Home Telephone: 301-837-3500 (Local) or 1-800-786-2551 (toll-free)

FAX: 301-837-3197

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 [OIG Contractor Reporting Form | Office of Inspector General OIG](#)