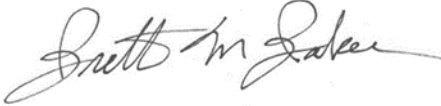




Inspector General

November 14, 2022

TO: Debra Steidel Wall
Acting Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General 

SUBJECT: *Audit of NARA's Fiscal Year 2022 Consolidated Financial Statements*
OIG Report No. 23-AUD-01

The Office of Inspector General (OIG) contracted with CliftonLarsonAllen, LLP (CLA) to conduct an independent audit on the financial statements of the National Archives and Records Administration (NARA) as of and for the fiscal years ended September 30, 2022 and 2021. The report should be read in conjunction with NARA's financial statements and notes to fully understand the context of the information contained therein.

CLA is responsible for the attached auditor's report dated November 10, 2022 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of CLA. 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

CLA issued an unmodified opinion on NARA's fiscal years 2022 and 2021 financial statements. CLA found:

- NARA's financial statements as of and for the fiscal years September 30, 2022 and 2021 are presented fairly, in all material respects, in accordance with United States Generally Accepted Accounting Principles;
- No material weaknesses, but one significant deficiency for FY 2022 internal controls over financial reporting based on limited procedures performed; and
- No reportable instances of noncompliance for fiscal year 2022 with provisions of applicable laws, regulations, contracts and grant agreements tested, and no other matters.

The report contains 20 recommendations to improve NARA's internal controls over financial reporting related to the significant deficiency in information technology controls. Management concurred with all of the recommendations. Based on your November 8, 2022 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 CLA and my staff during the audit. Please contact me or Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachment

cc: Micah Cheatham, Chief of Management and Administration
William Bosanko, Chief Operating Officer
Colleen Murphy, Chief Financial Officer and Senior Accountable Official
Sheena Burrell, Chief Information Officer
Meghan Guthorn, Deputy Chief Operating Officer
Kimm Richards, Accountability
Jewel Butler, Assistant Inspector General for Audits
Carol Seubert, Senior Financial Auditor
Kimberly Nikraves, Senior Program Auditor
United States Senate Homeland Security and Governmental Affairs Committee
United States House of Representatives Committee on Oversight and Reform



INDEPENDENT AUDITORS' REPORT

To: Inspector General
National Archives and Records Administration

Acting Archivist of the United States
National Archives and Records Administration

In our audits of the fiscal years (FYs) 2022 and 2021 financial statements of the National Archives and Records Administration (NARA), we found:

- NARA's financial statements as of and for the FYs ended September 30, 2022, and 2021, are presented fairly in all material respects, in accordance with United States of America (U.S.) generally accepted accounting principles;
- No material weakness, but a significant deficiency for FY 2022 internal control over financial reporting based on the limited procedures we performed; and
- No reportable noncompliance for FY 2022 with provisions of applicable laws, regulations, contracts, and grant agreements we tested and no other matters.

The following sections discuss in more detail (1) our report on the financial statements, which includes required supplementary information (RSI)¹, and other information (OI)² included in the Agency Financial Report; (2) our report on internal control over financial reporting; (3) our report on compliance with laws, regulations, contracts, and grants agreements and other matters; and (4) NARA's response to our findings and recommendations.

Report on the Audit of the Financial Statements

Opinion

We have audited the accompanying financial statements of NARA, which comprise the balance sheets as of September 30, 2022, and 2021; the related statements of net cost, changes in net position, and budgetary resources for the fiscal years then ended; and the related notes to the financial statements.

In our opinion, the National Archives and Records Administration's financial statements referred to above present fairly, in all material respects, NARA's financial position as of September 30, 2022, and 2021, and its net cost of operations, changes in net position, and budgetary resources for the FYs then ended in accordance with U.S. generally accepted accounting principles.

¹ The RSI consists of Management's Discussion and Analysis (MD&A), Deferred Maintenance and Repairs, and the Schedule of Budgetary Resources by Major Budget Accounts, which are included with the financial statements.

² Other Information consists of information included with the financial statements, other than RSI and the independent auditors' report.

Basis for Opinion

We conducted our audits in accordance with U.S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 22-01). Our responsibilities under those standards are further described in the Auditors' Responsibilities for the Audit of the Financial Statements section 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 audits. 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

NARA's management is responsible for (1) the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; (2) preparing, measuring, and presenting RSI in accordance with U.S. generally accepted accounting principles; (3) preparing and presenting other information included in the AFR, and ensuring the consistency of that information with the audited financial statements and the RSI; and (4) designing, implementing and maintaining effective internal control over financial reporting, including the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatements, 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 of financial statements conducted in accordance with *Government Auditing Standards* will always detect a material misstatement or a material weakness 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 to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

In performing an audit in accordance with *Government Auditing Standards*, 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 our audit of the financial statements 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

U.S. generally accepted accounting principles issued by the Federal Accounting Standards Advisory Board (FASAB) require that the RSI be presented to supplement the financial statements. Such information is the responsibility of management and, although not a part of the financial statements, is required by FASAB, which considers it to be an essential part of financial reporting for placing the financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the RSI in accordance with *Government Auditing Standards*, which consisted of inquiries of management about the methods of preparing the RSI and comparing the information for consistency with management's responses to the auditors' inquiries, the financial statements, and other knowledge we obtained during the audits of the financial statements, in order to report omissions or material departures from FASAB 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. NARA's management is responsible for the other information included in the AFR. The other information does not include the financial statements and our auditors' 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.

Report on 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 auditor's responsibilities discussed below.

Results of Our Consideration of Internal Control over Financial Reporting

Our consideration of internal control was for the limited purpose described above 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 and therefore, material weaknesses or significant deficiencies may exist that were not identified. 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. We identified certain deficiencies in internal control over financial reporting that we consider to be a significant deficiency, described below and in Exhibit A.

Longstanding Control Deficiency in Information Technology (IT) Controls

NARA did not substantially address deficiencies in its IT general control categories of security management, access controls, and configuration management that have existed since FY 2008. These longstanding unresolved deficiencies impact the effectiveness of NARA's information technology 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 deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that even if the control operates as designed the control objective would not be met. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively. A *material weakness* is a deficiency, or a 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 2022 audit, we identified additional 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 *Government Auditing Standards*.

Responsibilities of Management for Internal Control over Financial Reporting

NARA's management is responsible for (1) 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; (2) evaluating the effectiveness of internal control over financial reporting based on the criteria established under 31 U.S.C. 3512 (c), (d) (commonly known as the Federal Managers' Financial Integrity Act (FMFIA)); and (3) providing an assurance statement on the overall effectiveness of internal control over financial reporting included in management's discussion and analysis (MD&A).

Auditors' Responsibilities for the Consideration of Internal Control over Financial Reporting

In planning and performing our audit of NARA's financial statements as of and for the FY ended September 30, 2022, in accordance with *Government Auditing Standards*, 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 or on management's assurance statement on the overall effectiveness on internal control over financial reporting. Accordingly, we do not express an opinion on NARA's internal control over financial reporting or on management's

assurance statement on the overall effectiveness on internal control over financial reporting. We are required to report all deficiencies that are considered to be material weaknesses or significant deficiencies. We did not consider or evaluate all internal controls relevant to operating objectives as broadly established by the FMFIA, 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.

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 *Government Auditing Standards* in considering internal control over financial reporting. Accordingly, this report on internal control over financial reporting is not suitable for any other purpose.

Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements 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 auditor's responsibility 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 instance of noncompliance or other matters for FY 2022 that would be reportable under *Government Auditing Standards*. 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 *Government Auditing Standards*. Our responsibilities under those standards are further described in the Auditors' Responsibilities for Tests of Compliance section below.

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

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

Auditors' Responsibilities for Compliance with Laws, Regulations, Contracts and Grant Agreements and Other Matters

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.

Purpose of Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements 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 *Government Auditing Standards* in considering compliance. Accordingly, this report on compliance with laws, regulations, contracts, and grant agreements is not suitable for any other purpose.

Status of Prior Year's Control Deficiencies and Noncompliance Issues

We have reviewed the status of NARA's corrective actions with respect to the recommendations included in the prior year's Independent Auditors' Report, dated November 8, 2021. The status of prior year recommendations is presented in Exhibit C.

NARA's Response to Audit Findings and Recommendations

Government Auditing Standards requires the auditor to perform limited procedures on NARA's response to the findings and recommendations identified in our report and described in Exhibit B. NARA's response was not subjected to the auditing procedures applied in the audits of the financial statements and, accordingly, we express no opinion on the response.

CliftonLarsonAllen LLP



Greenbelt, MD
November 10, 2022

EXHIBIT A
Significant Deficiency
FY 2022

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

NARA relies extensively on information technology (IT) systems to accomplish its mission and in the preparation of 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 deficiencies in its IT general control categories of security management, access controls, and configuration management that have existed since FY 2008. These longstanding unresolved control deficiencies impact the effectiveness of NARA's IT security program and internal controls over financial reporting.

A summary of key findings related to the NARA Network (NARANet), Records Center Processing Billing System (RCPBS), and Order Fulfillment and Accounting System (OFAS) are categorized and listed by general control category as follows:

Access Controls – We found prior year weaknesses related to inactive user accounts, user account reviews, system access request procedures, multi factor user authentication, and identity and access management policy or strategy, remained unresolved. Access controls should be established to ensure user accounts are effectively managed.

Security Management – We found prior year weaknesses related to plan of action and milestones (POA&Ms) management, security plans, security assessment and authorization documentation not reviewed when there was a change in Authorizing Official (AO), controls not being tested, or security documentation was incomplete, remained unresolved. Security management controls provide the framework for the continual assessment of risk, development of security procedures, and monitoring the implementation effectiveness of those procedures.

Configuration Management – We found prior year unresolved weaknesses related to the detection, remediation, and monitoring of high and critical risk vulnerabilities for software patches and updates, and system configuration weaknesses which existed on NARA systems, and were publicly known since 2021 or earlier, still exist. In addition, we found prior year unresolved weaknesses related to configuration management plans and policies, baseline management procedures, and configuration-controlled changes which were not consistently maintained. The IT control deficiencies resulted from an ineffective patch and vulnerability management program, not prioritizing the development of organization wide configuration management policies and procedures, 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 financial information may be inadvertently or deliberately disclosed, manipulated, or misappropriated.

Contingency Planning – We found prior year unresolved weaknesses related to the testing of contingency plans. Although tests were conducted, they were not commensurate with the availability risk level of the information system. This IT control deficiency resulted from inconsistent NARA requirements for contingency plan testing, as well as inadequate oversight by NARA management.

Contingency planning controls provide reasonable assurance that contingency planning 1) protects information resources and minimizes the risk of unplanned interruptions and 2) provides for recovery of critical operations should interruptions occur.

Our testing was based 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-2 Account Management
Creates, enables, modifies, disables, and removes accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria].
- CA-5 Plans of Action and Milestones
Develops POA&Ms for the system to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and updates existing POA&Ms [Assignment: organization-defined frequency] based on the findings from controls assessments, independent audits or reviews, and continuous monitoring activities.
- CA-6 Security Authorization
Updates the authorizations [Assignment: organization defined frequency].
- PM-10 Authorization Process
Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes.
- 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
Replaces system components when support for the components is no longer available from the developer, vendor, or manufacturer.

- CM-1 Policy and Procedures
Develop, document, and disseminate to [Assignment: organization-defined personnel or roles) a configuration management policy that addresses, purpose, scope, roles, responsibilities, management commitment, coordination among organization entities and compliance and is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines, and procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls.
- CM-6 Configuration Settings
Establish, document, and implement 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]. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- CP-4 Contingency Plan Testing
Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].

NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*:

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities in an actual emergency situation, but in a simulated manner.

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 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.

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 repeat recommendations:

1. Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements.
2. 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.
3. Ensure system access requests are completed and retained for the duration of a users' system access.
4. Ensure account reviews are completed in accordance with Access Control IT Methodology requirements.
5. Enforce mandatory Personal Identity Verification (PIV) card authentication for all NARANet users, in accordance with OMB requirements.
6. Ensure system owners and Information System Security Officers (ISSO) have completed an E-Authentication Threshold Analysis (ETA) for all information systems with a signed E-Authentication Risk Assessment (if required).
7. Review and reduce the number of NARA users assigned to the PIV debarment group and move to the PIV mandatory group, using a risk-based decision process.
8. Continue and complete efforts to require PIV authentication for all privileged users, servers, and applications, through NARA's ██████████ authentication project and other efforts.
9. 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.
10. Ensure POA&Ms for the NARANet, RCPBS, and OFAS systems are created, updated, and remediated, for each system in accordance with NARA policies, guidance, and directives, to include enhanced POA&M closure procedures.
11. For those systems identified in which the Authorizing Official (AO) listed in the Authorization to Operate (ATO) has changed, NARA should follow the NARA Security Methodology for Certification and Accreditation (C&A) and Security Assessment in regard to requirements upon changes in authorizing officials. This is a separate activity from the ongoing authorization process.

12. Update NARA's Cyber Security Framework Methodology Processes & Procedures, for ongoing authorizations, to include examples of situations where a change in status could prompt the independent security control assessor to recommend re-certification of a system.
13. Develop oversight mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated prior to including in the plan.
14. Document and implement a process to track and remediate persistent configuration vulnerabilities, or document acceptance of the associated risks.
15. 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.
16. Fully complete the migration of applications to vendor supported operating systems.
17. Document, communicate, and implement NARA's configuration management processes applicable to all NARA systems, not just those under Information Services Enterprise Change Advisory Board (ECAB) control within for example, NARA's Configuration Management (CM) program management plan or other NARA methodology.
18. Finalize and implement system configuration baseline management procedures, which encompass at a minimum, the request, documentation, and approval of deviations from baseline settings for all NARA systems.
19. Ensure that records of configuration-controlled changes are retained within those systems (e.g., Remedy/ ServiceNow) which retain those records, in accordance with the NARA records schedule.
20. In coordination with system owners and ISSOs, identify and remediate inconsistencies in contingency plan testing requirements between the NARA Cyber Security Framework Methodology: Processes and Procedures and the NARA IT Security Methodology for Contingency Planning, to ensure requirements are more clearly defined and consistently communicated. As needed, NARA will then update contingency plan testing to commensurate with the availability risk level assigned.

EXHIBIT B
NARA's Response to our Findings and Recommendations
FY 2022



Archivist of the
United States

Date: November 8, 2022

To: Dr. Brett M. Baker
Inspector General

From: Debra Steidel Wall
Acting Archivist of the United States

Subject: Management Response to the FY2022 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, 2022.

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 CliftonLarsonAllen LLP for their cooperative and professional approach in the conduct of this audit.

Debra Steidel Wall

DEBRA STEIDEL WALL
Acting Archivist of the United States

EXHIBIT C
Status of Prior Year Recommendations

Our assessment of the current status of the recommendations related to findings identified in the prior year audit is presented below:

<i>FY 2021 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2022 Status</i>
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:		
1. Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements.	Significant Deficiency (SD)	Open; see 2022 Significant Deficiency, recommendation "A.1"
2. 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.	SD	Open; see 2022 Significant Deficiency, recommendation "A.2."
3. Ensure system access requests are completed and retained for the duration of a users' system access.	SD	Open; see 2022 Significant Deficiency, recommendation "A.3."
4. Ensure the completion and retention of exit clearance forms and requests for all separated employees, in accordance with NARA's record retention requirements.	SD	Closed
5. Ensure account reviews are completed in accordance with Access Control IT Methodology requirements.	SD	Open; see 2022 Significant Deficiency, recommendation "A.4."
6. Enforce mandatory Personal Identity Verification (PIV) card authentication for all NARANet users, in accordance with OMB requirements.	SD	Open; see 2022 Significant Deficiency, recommendation "A.5."
7. Ensure system owners and Information System Security Officers (ISSO) have completed an E-Authentication Threshold Analysis (ETA) for all information systems with a signed E-Authentication Risk Assessment (if required).	SD	Open; see 2022 Significant Deficiency, recommendation "A.6."
8. Review and reduce the number of NARA users assigned to the PIV debarment group and move to the PIV mandatory group, using a risk-based decision process.	SD	Open; see 2022 Significant Deficiency, recommendation "A.7."

<i>FY 2021 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2022 Status</i>
9. Continue and complete efforts to require PIV authentication for all privileged users, servers, and applications, through NARA's CyberArk authentication project and other efforts.	SD	Open; see 2022 Significant Deficiency, recommendation "A.8."
10. 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.	SD	Open; see 2022 Significant Deficiency, recommendation "A.9."
11. Ensure POA&Ms for the NARANet, RCPBS, and OFAS systems are created, updated, and remediated, for each system in accordance with NARA policies, guidance, and directives, to include enhanced POA&M closure procedures.	SD	Open; see 2021 Significant Deficiency, recommendation "A.10."
12. For those systems identified in which the Authorizing Official (AO) listed in the Authorization to Operate (ATO) has changed, NARA should follow the NARA Security Methodology for Certification and Accreditation (C&A) and Security Assessment in regard to requirements upon changes in authorizing officials. This is a separate activity from the ongoing authorization process.	SD	Open; see 2022 Significant Deficiency, recommendation "A.11."
13. Update NARA's Cyber Security Framework Methodology Processes & Procedures, for ongoing authorizations, to include examples of situations where a change in status could prompt the independent security control assessor to recommend re-certification of a system.	SD	Open; see 2022 Significant Deficiency, recommendation "A.12."
14. Develop oversight mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated prior to including in the plan.	SD	Open; see 2022 Significant Deficiency, recommendation "A.13."
15. Document and implement a process to track and remediate persistent configuration vulnerabilities, or document acceptance of the associated risks.	SD	Open; see 2022 Significant Deficiency, recommendation "A.14."

<i>FY 2021 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2022 Status</i>
16. 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.	SD	Open; see 2022 Significant Deficiency, recommendation "A.15."
17. Fully complete the migration of applications to vendor supported operating systems.	SD	Open; see 2022 Significant Deficiency, recommendation "A.16."
18. Document, communicate, and implement NARA's configuration management processes applicable to all NARA systems, not just those under Information Services Enterprise Change Advisory Board (ECAB) control within for example, NARA's Configuration Management (CM) program management plan or other NARA methodology.	SD	Open; see 2022 Significant Deficiency, recommendation "A.17."
19. Finalize and implement system configuration baseline management procedures, which encompass at a minimum, the request, documentation, and approval of deviations from baseline settings for all NARA systems.	SD	Open; see 2022 Significant Deficiency, recommendation "A.18."
20. Ensure that records of configuration-controlled changes are retained within those systems (e.g., Remedy/ ServiceNow) which retain those records, in accordance with the NARA records schedule.	SD	Open; see 2022 Significant Deficiency, recommendation "A.19."
21. In coordination with system owners and ISSOs, identify and remediate inconsistencies in contingency plan testing requirements between the NARA Cyber Security Framework Methodology: Processes and Procedures and the NARA IT Security Methodology for Contingency Planning, to ensure requirements are more clearly defined and consistently communicated. As needed, NARA will then update contingency plan testing to commensurate with the availability risk level assigned.	SD	Open; see 2022 Significant Deficiency, recommendation "A.20."
We recommend that NARA management implement the following recommendations:		
22. The Chief Financial Officer update the travel policy and continue efforts to ensure that all written policies and procedures are reviewed and revised timely.	Management Letter Comment (MLC)	Open; reclassified from SD in FY 2020 to MLC in FY 2021

<i>FY 2021 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2022 Status</i>
23. The Office of Chief Acquisition Officer ensures Contracting Officers understand their responsibility to use appropriate cost allocations for each contract line. (modified repeat recommendation)	MLC	Closed
24. The Chief Financial Officer updates Interim Guidance 400-8, <i>Quarterly Reconciliation of Open Items for all NARA Funds</i> , to include a review of open obligations for completeness. There should be steps for contracting officer representatives and program office management to take if they detect an obligation is not complete, including how to bring any errors to the attention of the Office of the Chief Financial Officer. (modified repeat recommendation)	MLC	Open; reclassified from SD in FY 2020 to MLC in FY 2021
25. The NARA Chief Financial Officer reports the Antideficiency Act (ADA) violation in accordance with Title 31, Section 1351 of the U.S. Code and OMB guidance.	Non-Compliance	Open Recommendation not repeated ³

³ Auditors' recommendation for NARA to report the ADA violation on the over-obligation in FY 2019 in the form of a letter from the agency head to the President through the Director of OMB (OMB Circular No. A-11, section 145.7, *How do I report a violation?*) is still open in FY 2022. NARA management stated that a draft letter was submitted to OMB in FY 2020, but NARA is still awaiting OMB's approval for NARA to finalize and issue the letter.