



November 14, 2017

TO: Colleen Murphy
Chief Financial Officer
Office of the Chief Financial Officer

FROM: James Springs *James Springs*
Inspector General

SUBJECT: *Audit of National Archives and Records Administration's
Fiscal Year 2017 Consolidated Financial Statements (Report No. 18-AUD-03)*

This memorandum transmits the results of the audit of the National Archives and Records Administration's (NARA) financial statements for fiscal years 2017 and 2016; and the results of the Office of Inspector General's (OIG) oversight of the audit and review of that report. The reports should be read in conjunction with NARA's financial statements and notes to fully understand the context of the information contained therein.

We contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (CLA) to audit NARA's financial statements as of September 30, 2017 and 2016, and for the years then ended. The contract required the audit be performed in accordance with U.S. generally accepted government auditing standards and Office of Management and Budget Bulletin 17-03, *Audit Requirements for Federal Financial Statements*.

Results of the Independent Audit

CLA issued an unmodified opinion on NARA's FY 2017 and 2016 financial statements. CLA found:

- The fiscal years 2017 and 2016 financial statements 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;
- One significant deficiency in internal control over financial reporting related to information technology controls; and
- No instances of noncompliance with certain provisions of laws, regulations, contracts and grant agreements.

Evaluation and Monitoring of Audit Performance

CLA is responsible for the attached auditor's report dated November 9, 2017, and the conclusions expressed in the accompanying reports. To ensure the quality of the audit work performed, we evaluated the independence, objectivity, and qualifications of the auditors and specialists; reviewed the plan and approach of the audit; monitored the performance of the audit; reviewed CLA's reports and related audit documentation; and inquired of its representatives. Our review, as differentiated from an audit in accordance with U.S. generally accepted government auditing standards, was not intended to enable us to express, as we do not express, an opinion on the financial statements or conclusions about the effectiveness of internal control over financial reporting or compliance with laws and regulations. Our review disclosed no instances where CLA did not comply, in all material respects, with generally accepted government auditing standards.

The report contains one recommendation(s) aimed at improving NARA's information technology controls. Your office concurred with the recommendation(s). Based on your November 9, 2017 response to the draft report, we consider all the recommendation(s) open. Once your office has fully implemented the recommendation(s), please submit evidence of completion of agreed upon corrective actions so that recommendation(s) may then be closed.

Your response to the draft report is attached. As with all OIG products, we will determine what information is publically 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. In addition, we will post a copy of the report on our public website.

I appreciate the cooperation and assistance NARA extended to CLA and my staff during the audit. Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.

Attachment



CliftonLarsonAllen

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

INDEPENDENT AUDITORS' REPORT

Inspector General
National Archives and Records Administration

Archivist of the United States
National Archives and Records Administration

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the National Archives and Records Administration (NARA), which comprise the consolidated balance sheets as of September 30, 2017 and 2016, and the related consolidated statements of net cost and changes in net position, the combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements (financial statements).

Management's Responsibility for the Financial Statements

NARA management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America (U.S.); this includes the design, implementation, and maintenance of 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' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the U.S.; 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. 17-03, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 17-03). Those standards and OMB Bulletin 17-03 require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation 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 the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the National Archives and Records Administration as of September 30, 2017 and 2016, and its net costs, changes in net position, and budgetary resources for the years then ended, in accordance with accounting principles generally accepted in the U.S.

Other Matters

Required Supplementary Information

Accounting principles generally accepted in the U.S. require that the information in the NARA's Management Discussion and Analysis and other Required Supplementary Information be presented to supplement the financial statements. Such information, although not a part of the financial statements, is required by the Federal Accounting Standards Advisory Board, who 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 required supplementary information in accordance with auditing standards generally accepted in the U.S., which 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 financial statements, and other knowledge we obtained during our audits of the financial statements. We do not express an opinion or provide any assurance on this information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audits were conducted for the purpose of forming an opinion on the financial statements as a whole. The Letter from the Archivist of the United States, the Letter from the Chief Financial Officer, and the Other Information in Section 3 of the Agency Financial Report are presented for purposes of additional analysis and are not a required part of the financial statements. This information has not been subjected to the auditing procedures applied in the audits of the financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Report on Internal Control over Financial Reporting and on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered NARA's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control or on management's statement of assurance on internal control included in the MD&A. Accordingly, we do not express an opinion on the effectiveness of NARA's internal control or on management's statement of assurance on internal control included in the Management's Discussion and Analysis.

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 a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of NARA's financial statements will not be prevented, or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies 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 that we consider to be material weaknesses. However, we identified a deficiency in internal control, described below and in Exhibit A that we consider to be a significant deficiency.

Longstanding Control Deficiency in Information Technology Controls

NARA did not substantially address information technology control deficiencies that have existed since FY2008. NARA not addressing these longstanding unresolved deficiencies impacts the effectiveness of NARA's information security program and internal controls over financial reporting. NARA did make some progress to mitigate these deficiencies but more effort is needed.

Compliance

As part of obtaining reasonable assurance about whether NARA's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements noncompliance with which could have a direct effect on the determination of material financial statement amounts and disclosures. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion.

The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported in accordance with *Government Auditing Standards* or OMB Bulletin 17-03.

Management's Responsibility for Internal Control and Compliance

Management is responsible for (1) evaluating the effectiveness of internal control over financial reporting based on criteria established under the Federal Managers Financial Integrity Act (FMFIA) (2) providing a statement of assurance on the overall effectiveness on internal control over financial reporting, and (3) complying with other applicable laws, regulations, contracts, and grant agreements.

Auditors' Responsibilities

We are responsible for: (1) obtaining a sufficient understanding of internal control over financial reporting to plan the audit and (2) testing compliance with certain provisions of laws, regulations, contracts, and grant agreements.

We did not evaluate all internal controls relevant to operating objectives as broadly established by the FMFIA, such as those controls relevant to preparing statistical reports and ensuring efficient operations. We limited our internal control testing to testing controls over financial reporting. Because of inherent limitations in internal control, misstatements due to error or fraud, losses, or noncompliance may nevertheless occur and not be detected. We also caution that projecting our audit results to future periods is subject to risk that controls may become inadequate because of changes in conditions or that the degree of compliance with controls may deteriorate. In addition, we caution that our internal control testing may not be sufficient for other purposes.

We did not test compliance with all laws, regulations, contracts and grant agreements applicable to NARA. We limited our tests to certain provisions of laws, regulations, contracts and grant agreements noncompliance with which could have a direct effect on the determination of material financial statement amounts and disclosures. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. We caution that noncompliance may occur and not be detected by these tests and that such testing may not be sufficient for other purposes.

Management's Response to Findings

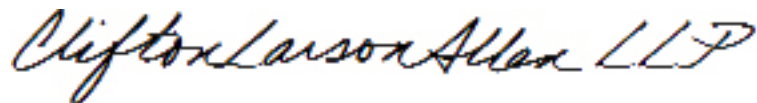
Management's response to the findings identified in our report is presented in Exhibit B. We did not audit NARA's response and, accordingly, we express no opinion on it.

Status of Prior Year's Control Deficiencies and Noncompliance Issues

We have reviewed the status of NARA's corrective actions with respect to the findings included in the prior year's Independent Auditors' Report, dated November 10, 2016. The status of prior year findings is presented in Exhibit C.

Purpose of the Report on Internal Control over Financial Reporting and the Report on Compliance

The purpose of the Report on Internal Control over Financial Reporting and on Compliance is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of NARA internal control or on compliance. These reports are an integral part of an audit performed in accordance with *Government Auditing Standards* in considering NARA's internal control and compliance. Accordingly, this report is not suitable for any other purpose.



CliftonLarsonAllen LLP

Arlington, Virginia
November 9, 2017

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 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's staff use IT systems to initiate and authorize financial transactions at the workstations, which transmit those transactions across the network to servers that record, process, summarize, and report financial transactions that support the preparation of its financial statements.

In the prior year, we reported a significant deficiency in information technology controls which identified control deficiencies in five IT general control categories including access controls, security management, contingency planning, segregation of duties, and configuration management.

In the current fiscal year, NARA did make some progress to mitigate these deficiencies but more effort is needed. 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.

These weaknesses could be potentially exploited, intentionally or unintentionally, to undermine the integrity and completeness of data processed by NARA's financial management systems, including those systems which feed into or are reconciled with data processed by the Records Center Program Billing System (RCPBS) and Order Fulfillment and Accounting System (OFAS) systems. We also continued to note control weaknesses for the NARA Network (NARANet), and Visitor Services Reservation Scheduling System (VISTA) systems.

A summary of key findings related to NARANet, OFAS, VISTA and RCPBS systems are categorized and listed by general control category as follows:

Access Controls – We found prior year unresolved weaknesses related to the transmission of passwords in clear text (not encrypted) for an internal website, continued to identify instances (although a reduced number compared to FY2016) of inactive and duplicate user accounts, and securing access to sensitive areas. Access controls should be established to ensure passwords and user authentication credentials are transmitted securely, user accounts are more effectively managed and access to sensitive areas is restricted to authorized individuals.

Security Management – We found prior year unresolved weaknesses related to system security plans which were incomplete or not current. Additionally, during FY 2017, we found that plans of actions and milestones (POA&Ms) were not updated timely, missed milestone dates or contained incomplete data. Security management controls should be established which provide the framework for the continual assessment of risk, developing and implementing effective security procedures and monitoring the effectiveness of those procedures.

Configuration Management – We found that while there were improvements in this area compared to FY2016, configuration management weaknesses associated with vulnerability and patch management, continue to be identified. Specifically, we found prior year unresolved weaknesses related to the monitoring, detecting, and remediating known vulnerabilities for software patches and updates. Additionally, system configuration weaknesses existed on servers

and workstations. Effective vulnerability management reduces the risk of incurring a breach and decreases the time and effort necessary to appropriately respond after a breach.

Our testing was based on the following key criteria:

- NARA IT Security Requirements
 - IA-5(1) For all data, the information system, shall, for password-based authentication: Stores and transmits only encrypted representations of passwords.
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*”
 - SI-2 Flaw Remediation
The organization identifies information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.
 - SA-22 Unsupported System Components
The organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer;
 - CA-5 Plans of Action and Milestones
The organization develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
- OMB Circular A-130, Appendix I, *Management of 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 the National Institute of Standards and Technology (NIST).

The IT control deficiencies resulted from an ineffective implementation and oversight by NARA management of key controls over security management, access controls, and configuration management controls. While management was in the process of deploying an Information System Security Officer (ISSO) contract to remediate these weaknesses, these efforts were still ongoing during FY2017.

Recommendations:

- 1) We recommend that the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to:
 - a. Strengthen controls for internal website password transmission and encryption to include Hyper Text Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) technologies.
 - b. Strengthen the review and disabling of user accounts in accordance with NARA's information technology policies and requirements.
 - c. Implement enhanced processes to secure physical access controls to sensitive areas.
 - d. Continue to implement improved processes for reviewing and updating key security documentation, including system security plans on an annual basis.
 - e. Implement improved processes for creating, updating and remediating plans of actions and milestones.
 - f. Implement remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure.
 - g. Fully complete the migration of applications to vendor supported operating systems.

EXHIBIT B
Management's Response



NATIONAL
ARCHIVES

ARCHIVIST *of the*
UNITED STATES

DAVID S. FERRIERO

T: 202.357.5900

F: 202.357.5901

david.ferriero@nara.gov

Date: November 9, 2017
To: James Springs
Inspector General
From: David S. Ferriero
Archivist of the United States
Subject: Management Response to the FY2017 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, 2017.

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 Security challenges identified in this report and concurs with the recommendation of the independent auditor. NARA self-identified IT security as a material weakness in internal controls and a summary of our corrective action plan is included in the FY 2017 Statement of Assurance. I appreciate the work performed by the auditor in this area and will ensure the auditor's findings and recommendation 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.

DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

700 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20408-0001

www.archives.gov

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 2016 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2017 Status</i>
<p>1. Develop and execute a realistic holistic IT plan with target dates to resolve longstanding issues over access controls, security management, contingency planning, segregation of duties, and configuration management.</p>	<p>Significant Deficiency (SD) 2016</p>	<p>Closed</p>
<p>2. NARA CIO continues to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to:</p> <ul style="list-style-type: none"> a. Implement improved processes to ensure the timely removal of system access for separated employees and strengthen Supervisor training related to the employment separation process. b. Implement improved processes for the periodic review of network and financial applications to identify and remove inactive accounts on systems and networks. Recertify that access remains appropriate and is restricted to necessary personnel. c. Implement enhanced processes to secure physical access controls to sensitive areas. d. Implement a process for monitoring network audit logs for unauthorized or unusual activities. Implement procedures for analyzing network audit logs and ensuring such logs are maintained in accordance with NARA policy. e. Implement processes to ensure that default and easy to guess passwords are changed and all passwords are transmitted securely and encrypted. f. Implement improved processes for reviewing and updating key security documentation, including system security plans on an annual basis. Such updates will ensure all required information is included and accurately reflects the current environment, new security risks, and applicable federal standards. g. Implement improved processes for user account management to ensure assigned user permissions are commensurate with assigned position responsibilities. 	<p>Significant Deficiency (SD) 2016</p>	<p>Partially Closed: see 2017 Significant Deficiency</p> <p>The following recommendations were still identified as being open during FY2017; c, e, f, h and i</p>

EXHIBIT C
Status of Prior Year Recommendations

<i>FY 2016 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2017 Status</i>
h. Strengthen patch and vulnerability management program to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure. i. Fully complete the migration of applications to vendor supported operating systems. j. Implement improved change control procedures to ensure the consistent testing of system changes for NARA financial applications.		