WILLIAMS ADLEY

MANAGEMENT LETTER

Inspector General, National Endowment for the Arts
Chairman, National Endowment for the Arts

We have audited the balance sheet as of September 30, 2017 and 2016, and the related statements of net cost, changes in net position, and budgetary resources for the year then ended, hereinafter referred to as "financial statements", of the National Endowment for the Arts (NEA) and have issued an unmodified opinion thereon dated November 3, 2017.

In planning and performing our audit of the financial statements of the NEA, we considered its internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide assurance on internal control. We have not considered NEA's internal control since the date of our report.

In our fiscal year 2017 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We noted three matters in FY 2017 that are discussed in Appendix I and one matter from our FY 2016 audit that remains open. Additionally, we have provided the status of the prior year management letter comments in Appendix I.

We appreciate the cooperation and courtesies extended to us during the conduct of the audit. We will be pleased to meet with you or your staff, at your convenience, to discuss issues in this letter or furnish any additional information you may require.

Williams, Adley & Company-DC, LLP
Washington, District of Columbia
November 3, 2017

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

APPENDIX I
Deficiencies noted in FY2017 and Status of Prior Year Finding

The following are deficiencies noted during our audit of the FY2017 financial statements.

NFR #2017-01: Configuration Management Policy Needs to be Improved

Condition:

NEA's Configuration Management Policy lacks the following elements:

- Process for initiating a change request, to include form/document to be used
- A clear identification of roles and responsibilities for the following:
    - Individual Responsible for the review and approval of the change request
    - Individual responsible for the User Acceptance Testing
    - A system of records that would be used to capture change request life-cycle (from initiation to migration)

Cause:

Based on inquiries of NEA personnel, they heavily rely on service providers (i.e. NFC and ESC) to implement controls over the configuration management process.

NEA's management does not have a clear understanding of the NIST requirements and the Configuration Management Complementary User Entity Controls (CUEC) required by the SSAE 18 reports.

Effect:

Not having a clear and detailed Configuration Management Policy may prevent NEA from following a consistent process when reviewing and approving change request.

In addition, not having clear identification of roles and responsibilities (to include testing of changes) may increase the risk of introducing faulty changes into production due to an inadequate/insufficient quality control process.

Criteria:

NIST Special Publication 800-128 Chapter 3.1.1 states the following:

Develop Organizational security-focused configuration management (SecCM) Policy

The organization is typically responsible for defining documented policies for the SecCM program. The SecCM program manager develops, disseminates, and periodically reviews and updates the SecCM policies for the organization. The policies are included as a part of the overall organization-wide security policy. The SecCM policy normally includes the following:

- Purpose – the objective(s) in establishing organization-wide SecCM policy;

- Scope – the extent of the enterprise architecture to which the policy applies;
- Roles – the roles that are significant within the context of the policy;
- Responsibilities – the responsibilities of each identified role;
- Activities – the functions that are performed to meet policy objectives;
- Common secure configurations – federal and/or organization-wide standardized benchmarks for configuration settings along with how to address deviations; and
- Records – the records of configuration management activities to be maintained; the information to be included in each type of record; who is responsible for writing/keeping the records; and procedures for protecting, accessing, auditing, and ultimately deleting such records.

The Enterprise Services Center (ESC)[1] FY2017 SSAE 18 report requires NEA to implement the following CUEC:

"Controls to provide reasonable assurance that system changes are reviewed and tested and user acceptance documentation is timely returned to the ESC."

Recommendation:

We recommend that NEA revise the Configuration Management Policy to include:

- The process that should be followed to initiate a change request.
- Who is allowed to initiate change requests.
- The records that need to be maintained to provide evidence of all the phases of the change request (i.e. initiation, review/approval, testing, and migration). These records should indicate who would be involved and responsible for initiation, review/approval, testing and migration of change request.
- Clear roles and responsibilities of all the individuals that are part of the configuration management process.

Management Response:

NEA management concurred with the finding and noted that they will review the configuration management policy by March 30, 2018. See NEA's complete response in Appendix II.

Auditor Analysis:

We believe that the proposed action is sufficient to close the finding if properly implemented during FY2018.

[1] ESC host and operates NEA's accounting system Delphi.

NFR #2017-02: Property, Plant and Equipment Tracking

Condition:

NEA's tracking of accountable property and capitalized equipment could be improved. We noted the following exceptions during our testwork:

Accountable Assets
We selected five assets located at NEA headquarters and requested supporting documentation for them. NEA was unable to provide us with supporting documentation related to two of the five assets selected. Additionally, we could not trace these items to the capital assets listing.

Capitalized Assets
We randomly selected 10 items from the capital asset listing. We were not able to physically observe two (2) Uninterrupted Power Supply (UPS) power outlets capitalized ($298) with a phone system. This phone system and UPS items were installed at the prior NEA headquarters location. Per further inquiry of NEA, we noted that additional UPS items totaling $6,048, were also abandoned in NEA's prior headquarter location.

NEA explained that the UPS system items were abandoned in the NEA's old office when they moved to the Constitution Center location in 2014. NEA stated that GSA did not provide disposition/disposal documentation related to these items. NEA did not remove the items from the capitalized assets listing nor recorded their disposal.

Cause:

Accountable Assets
Per discussion with the Administrative Services Office (ASO) Director, ASO did not receive procurement documentation for the items during the inventory management transition in FY2016 from Information & Technology Management (ITM). Per our inquiries, ITM and ASO did not have any form of management-sanctioned policies and procedures in place for maintaining Accountable Property until September 11, 2017. This newly approved ASO accountable property inventory policy does not address record keeping policy.

Capitalized Assets
Per a memo dated June 30, 2016, ASO Director had knowledge that General Service Administration (GSA) was not able to produce any documentation concerning disposition of the items abandoned in-place in 2014 at the prior location. ASO did not communicate this information to the Office of Finance, which ultimately is responsible for removing disposed items from the accounting system.

Effect:

NEA's capitalized equipment listing is inaccurate because it includes asset items NEA does not currently possess and should no longer depreciate. Therefore, based on the testing of our sample items, we noticed that the PP&E balance included assets in the amount of $6,346 that should not have been included in the General Ledger Account 1750 as of June 30, 2017.

In addition, NEA ASO does not have defined policies and procedures related to record-keeping of accountable property documentation as they cannot provide support for ownership of the two items purchased in August 2016.

Criteria:

Federal Acquisition Regulation Subpart 4.8- Government Contract Files states the following in section 4.805:

(a) Agencies must prescribe procedures for the handling, storing, and disposing of contract files, in accordance with the National Archives and Records Administration (NARA) General Records Schedule 1.1, Financial Management and Reporting Records. The Financial Management and Reporting Records can be found at http://www.archives.gov/records-mgmt/grs.html. These procedures must take into account documents held in all types of media, including microfilm and various electronic media. Agencies may change the original medium to facilitate storage as long as the requirements of Part 4, law, and other regulations are satisfied. The process used to create and store records must record and reproduce the original document, including signatures and other written and graphic images completely, accurately, and clearly. Data transfer, storage, and retrieval procedures must protect the original data from alteration. Unless law or other regulations require signed originals to be kept, they may be destroyed after the responsible agency official verifies that record copies on alternate media and copies reproduced from the record copy are accurate, complete, and clear representations of the originals. When original documents have been converted to alternate media for storage, the requirements in Table 4-1 of this section also apply to the record copies in the alternate media.

Table 4.1 shows that contracts and records or documents should be retained 6 years after final payment.

NEA's Directive 1317- Record Management states the following about the ASO's responsibility:

1. Coordinate with the National Archives and Records Administration (NARA) to develop and maintain approved records disposition schedules.
2. Consult with the NEA's Chief Information Officer in developing Agency policies and procedures for electronic record management and the identification and protection of vital records.
3. Develop and maintain instructional guidance for the NEA records management and vital records program.

4. Ensure prompt retirement or disposal of temporary records and the timely transfer of permanent records in accordance with approved records disposition schedules.

Recommendation:

We recommend that NEA:

1. Revise the newly implemented ASO accountable property inventory policies and procedures to include a section addressing equipment record-keeping to ensure all necessary documentation is retained in the financial management system. NEA should ensure that this policy includes guidance on handling abandoned property and updating the capital asset listing for the property abandoned.
2. Revise capitalized property policies and procedures to provide specific guidelines for asset tracking, disposals, and additions.
3. Provide proper training to all staff involved with inventory management to ensure that policies and procedures in place are followed.
4. For the exceptions noted, ensure that the financial management system are updated with the appropriate documentation.
5. Update capitalized assets listing to reflect the appropriate items and dollar amount. In addition, NEA should reduce the PP&E GL account balance to exclude the assets abandoned in the old office.
6. Establish procedures for communicating with the Office of Finance any and all capitalized assets dispositions/abandonments in a timely manner.

Management Response:

NEA management concurred with the finding. They noted that they will update their policies and procedures and the capitalized asset listing. See NEA's complete response in Appendix II.

Auditor Analysis:

We believe that the proposed actions are sufficient to close the finding if properly implemented during FY2018.

<u>NFR #2017-03: Access Controls Observations- Information Systems Password Settings</u>

Condition:

NEA did not comply with their Password Policy document. Specifically, we received a screenshot dated July 26, 2017 of NEA's *Default Domain Policy* settings where it shows the aging of the password to be 90 days; however, the Password Policy states that it should be set to 60 days.

Also, we noticed that NEA did not comply with their Access Control Policy. Specifically, the policy states that a user should be locked out after three unsuccessful login attempts. Based on our

analysis of the login/password parameters, we noticed that the setting was set to five unsuccessful attempts and not three. Also, per our observation on September 29, 2017, we noticed that the Information System Security Officer (ISSO) was allowed five unsuccessful login attempts. The Information System Security Officer (ISSO) immediately corrected this.

Cause:

The ISSO did not detect this noncompliance during his audit of the information system. He believed that the password policy was compliant with the Access Control policy.

Effect:

Having less stringent password settings in place increases the risk of unauthorized access to NEA's network.

Criteria:

Section III of NEA's Password Policy states that passwords must be changed every 60 days. Also, section V of the Access Control Policy states the following, under the heading AC-7- Unsuccessful Logon Attempts:

"System Owners shall ensure that their information systems implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three within thirty-minute period."

Finally, section IV of the Access Control Policy notes that ISSO is responsible for auditing information systems to ensure compliance with the procedures and guidelines specified in the policy.

Recommendation:

We recommend that NEA:

1. ISSO perform a thorough review of their information system to ensure that it is consistent with the settings established in the written policies and procedures.

Management Response:

The NEA Office of Information & Technology stated that they will review and revise all access control and account management policies to align with one another by December 31, 2017. See NEA's complete response in Appendix II.

Auditor Analysis:

We believe that the finding can be closed if NEA implements the proposed actions and implements our recommendations in their entirety by FY2018.

Status of Prior Year Findings

NFR #2016-02: NEA did not conduct quarterly reviews of HR administrator webTA users (Repeat Condition)

Status:

In our FY 2016 audit, we noted that there was no documented review of the HR Administrator role in webTA. In FY 2017, NEA began documenting these reviews and was able to provide support for the review for the 1st quarter of fiscal year 2017. However, NEA did not perform the reviews for the 2nd and 3rd quarters of fiscal year 2017.

NEA's response has not been subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.

The following is the status of the prior year finding noted in the FY2016 management letter.

Prior Year Finding	**Current Year Status**
Improvements needed in the FBwT reconciliation approval process	Finding closed.
NEA is not documenting the periodic reviews of access privileges performed on the NFC webTA system	Partially closed. Refer to NFR #2016-02 above.

ART WORKS.

National Endowment for the Arts
arts.gov

November 7, 2017

Mr. Kola A. Isiaq, CPA
Managing Partner
Williams Adley & Company, LLP
1030 15th Street, NW, Suite 350 West
Washington, DC 20005

Dear Mr. Isiaq:

This is the NEA's response to your Management Letter of November 3, 2017, issued in connection with your audit of our FY 2017 and FY 2016 financial statements.

We are pleased with your issuing an unmodified opinion, and that you did not identify any material deficiencies in internal control over financial reporting. We are providing the following responses to the matters you noted in your management letter.

NFR #2017-01: Configuration Management Policy Needs to be Improved
Management concurs. NEA's Office of Information & Technology Management will continue to strengthen its information security program through the comprehensive review and revision of the configuration management policies and procedures by March 30, 2018.

NFR #2017-02: Property, Plant and Equipment Tracking

Management concurs. We will update the accountable property inventory policies and procedures to address the documentation that needs to be retained in related procurement files as required by year end Fiscal Year 2018. We will revise our capitalized property policies and procedures to provide specific guidelines for asset tracking, disposals, and additions during the current fiscal year. We will identify key staff involved in property management functions and provide training on agency accountable property inventory policies and procedures to establish consistent inventory management practices for agency property as required by the end of Fiscal Year 2018. For the exceptions noted, we were able to account for all five assets selected with the exception of procurement documentation for two assets. If and when we locate the relevant procurement documentation, the files will be updated accordingly. We will complete an adjustment to the capitalized assets listing to reflect the appropriate items and dollar amount during first quarter Fiscal Year 2018. We will establish procedures to facilitate appropriate and timely communication between the Administrative Services Office and the Finance Office concerning any and all capitalized assets dispositions and/or abandonments.

NFR #2017-03: Access Controls Observations - Information Systems Password Settings
Management concurs. NEA's Office of Information & Technology Management will continue to strengthen its information security program through the comprehensive review and revision, by December 31, 2017, of all access control and account management policies and procedures to align with one another.

NFR #2016-02: NEA did not conduct quarterly reviews of HR administrator webTA users (Repeat Condition)

Management concurs. The NEA acknowledges that, due to the absence of a Deputy Chairman for Management & Budget (DCMB) for 6 ½ months (April 2017 through mid-October 2017) and the subsequent interim delegation of various functions and authorities, review of the WEBTA Administrator roles and the WEBTA User roles was mistakenly overlooked. The NEA concurs with the original 2016 recommendation that the NEA ensure that the HR Administrator and WEBTA users are reviewed on a quarterly basis and that this review is documented. We agree that the review process should be performed by the DCMB or an appointed delegate from the DCMB office. Now that the position of the DCMB has been filled, this review process will continue to be conducted on a consistent quarterly basis, with safeguards implemented to ensure that the review process is not overlooked in the future.

Sincerely,

Ann C. Eilers
Deputy Chairman for Management and Budget
National Endowment for the Arts