JAMESTOWN-YORKTOWN FOUNDATION

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JULY 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

- TABLE OF CONTENTS -

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 22, 2023

Christy Coleman, Executive Director
Jamestown-Yorktown Foundation
2110 Jamestown Road
Williamsburg, Virginia 23185

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Jamestown-Yorktown Foundation** (Foundation). We completed the review on July 13, 2023. The purpose of this review was to evaluate if the agency has developed adequate internal controls over significant organizational areas and activities and not to express an opinion on the effectiveness of internal controls. Management of the Foundation is responsible for establishing and maintaining an effective control environment.

Review Process

During the review, the agency completes an Internal Control Questionnaire that covers significant organizational areas and activities including payroll and human resources; revenues and expenses; procurement and contract management; capital assets; grants management; debt; and information technology and security. The questionnaire focuses on key controls over these areas and activities.

We review the agency responses and supporting documentation to determine the nature, timing, and extent of additional procedures. The nature, timing, and extent of the procedures selected depend on our judgment in assessing the likelihood that the controls may fail to prevent and/or detect events that could prevent the achievement of the control objectives. The procedures performed target risks or business functions deemed significant and involve reviewing internal policies and procedures. Depending on the results of our initial procedures, we may perform additional procedures including reviewing evidence to ascertain that select transactions are executed in accordance with the policies and procedures and conducting inquiries with management. The "Review Procedures" section below details the procedures performed for the Foundation. The results of this review will be included within our risk analysis process for the upcoming year in determining which agencies we will audit.

Review Procedures

We evaluated the agency's corrective action for the 2020 internal control questionnaire review findings as well as the findings in the report titled "Cycled Agency Information Systems Security Review for the year ended June 30, 2020." The agency has taken adequate corrective action with respect to review findings reported in the prior review and audit that are not repeated in the "Review Results" section below.

We reviewed a selection of system and transaction reconciliations in order to gain assurance that the statewide accounting system contains accurate data. The definitive source for internal control in the Commonwealth is the Agency Risk Management and Internal Control Standards (ARMICS) issued by the Department of Accounts (Accounts); therefore, we also included a review of ARMICS. The level of ARMICS review performed was based on judgment and the risk assessment at the Foundation. Our review of the Foundation's ARMICS program included a review of all current ARMICS documentation and a comparison to statewide guidelines established by Accounts. Further, we evaluated the Foundation's process of completing and submitting attachments to Accounts.

We reviewed the Internal Control Questionnaire and supporting documentation detailing policies and procedures. As a result of our review, we performed additional procedures over the following areas: payroll and human resources; revenues and expenses; contract management; capital assets; and information technology and security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are effectively designed and implemented; reviewing transactions for compliance with internal and Commonwealth policies and procedures; and conducting further review over management's risk assessment process.

As a result of these procedures, we noted areas that require management's attention. These areas are detailed in the "Review Results" section below.

Review Results

We noted the following areas requiring management's attention resulting from our review:

- **Repeat -** The Foundation continues to not conduct risk assessments for all sensitive systems as required by the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Additionally, the Foundation does not conduct and document information technology (IT) system and data sensitivity classifications for its IT systems to determine which systems are sensitive, which would assist the Foundation in identifying which systems require a risk assessment. The Foundation should work with its external contractor to conduct IT system and data sensitivity classifications of the Foundation's IT systems to determine which systems are sensitive. Using the updated sensitive system list, the Foundation and its external contractor should complete risk assessments for its sensitive systems. Additionally, the Foundation should develop a plan to conduct annual self-assessments of its risk assessments to validate the information and update the risk assessments, as necessary. Completing risk assessments for its sensitive systems will assist

the Foundation in detecting risks and vulnerabilities to its sensitive IT environment to remediate and ensure the confidentiality, integrity, and availability of its sensitive and mission critical data.

- **Repeat -** The Foundation has not made progress since the prior audit of information systems security to implement certain audit logging and monitoring controls as required by the Security Standard. We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to the descriptions of security mechanisms. The Foundation should remediate the weaknesses discussed in the communication marked FOIAE in accordance with the Security Standard to protect the confidentiality, integrity, and availability of its sensitive and mission critical data.

- **Repeat -** The Foundation continues to not have appropriate controls in place to ensure that logical access to its systems complies with the requirements of the Security Standard and the Foundation's Logical Access Controls Policy. Specifically the Foundation does not have a formal process in place to conduct and document its review of systems access at least annually. In addition, the Foundation does not have a formal and consistent process in place to ensure that inactive accounts are disabled after 90 days of inactivity across its individual systems and applications. The Foundation should develop and implement procedures to support its Logical Access Controls Policy to ensure that the Foundation consistently applies adequate security controls for access reviews and removals. Additionally, the Foundation should implement the formal processes to it reviews, disables, and removes system access in accordance with the Logical Access Controls Policy and the Security Standard.

- **Repeat -** The Foundation has not made any progress in testing its IT Disaster Recovery Plan since our prior information systems security audit. While the previous audit found that the Foundation maintained a comprehensive Continuity Plan that included an adequate IT Disaster Recovery Plan, the Foundation continues to not annually test the IT Disaster Recovery Plan components. The Security Standard requires that agencies perform an annual exercise of IT Disaster Recovery components to assess their adequacy and effectiveness (*Security Standard, Section CP-1 Contingency Planning Policies and Procedures*). The Foundation should develop and implement a formal process to test its IT Disaster Recovery Plan, which will help protect the confidentiality, integrity, and availability of the agency's sensitive and mission critical data.

- **Repeat -** The Foundation continues to not have an adequate policy and consistent process to administer, monitor, or enforce annual security awareness training for all information system users in accordance with the Security Standard and Security Awareness Training Standard, SEC 527 (Security Awareness Training Standard). The Foundation should update its Security Awareness Policy and develop formal procedures to align with the requirements within the Security Standard and Security Awareness Training Standard. Additionally, the Foundation should improve its process and assign employees to security awareness training in a timely manner, which will assist in ensuring employees complete the training by the required

deadlines. The Foundation should also implement a process for monitoring and enforcing security awareness training completion which will help ensure the confidentiality, integrity, and availability of the Foundation's sensitive IT environment.

- **Repeat** – The Foundation has formal, documented policies and procedures over several significant business processes; however, we identified several areas in which policies and procedures were incomplete or outdated. Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures (CAPP) Manual require each agency to "publish its own policies and procedures documents, approved in writing by agency management." Management should ensure detailed policies and procedures exist for all critical business areas. In addition, management should continue to develop a formal process to review and approve all policies and procedures either annually or as needed and maintain documentation of the process.

- **Repeat** – The Foundation's ARMICS process covers most of the minimum requirements set by Accounts; however, we identified some requirements that the Foundation did not meet. The Foundation did not document the consideration of fraud risk or the assessment of the information and communication internal control component within the agency-level risk assessment. The Foundation did not perform transaction-level risk assessments on all significant fiscal processes identified. The Foundation also identified key controls for transaction-level review; however, there is no documentation of control testing to ensure the controls are functioning properly. The Foundation should update the ARMICS process to ensure it meets all minimum requirements.

- The Foundation is responsible for maintaining oversight of two current service providers but does not have a formal policy or process in place to maintain consistent oversight of the two service providers to ensure the service providers comply with the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard). The Foundation should develop a formal process to monitor and maintain oversight of its third-party providers to ensure they comply with the Hosted Environment Security Standard. Appropriate monitoring of third-party service providers helps maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

- The Foundation did not obtain the System and Organization Controls (SOC) report for a provider that processes sensitive information and as such did not document an evaluation of the SOC report and the complementary user entity controls described within the report. CAPP Manual Topic 10305 and the Security Standard require agencies to have an adequate level of interaction with third-party providers to obtain an understanding of the providers' internal control environments as well as any required complementary controls the agency would need to implement. Agencies must also maintain oversight of the provider to gain assurance over outsourced operations. The Foundation should develop policies and procedures for SOC reports and ensure it obtains and evaluates SOC reports timely.

- The Foundation did not evaluate all contracts to properly identify all potential leases in accordance with Governmental Accounting Standards Board (GASB) Statement No. 87. The Foundation also did not properly evaluate and record the group of leased assets with the same contracted vendor, lease term, and interest rate. In addition, the Foundation did not follow the correct procedure for determining the interest rate. CAPP Manual Topic 31200, which references GASB Statement No. 87, requires agencies to properly identify leases and group leases for recording in the lease accounting system to ensure proper classification of leases as long-term and short-term; and to evaluate explicit, implicit, and incremental borrowing rates before resorting to using the prime rate for a reasonable and accurate interest rate. Management should update lease processes and ensure it properly records and classifies leases.

- The Foundation did not remove critical administrator-level roles to the Commonwealth's human resource and payroll management system from four employees timely in accordance with the Foundation's updated separation of duties policy. The Foundation should ensure it consistently reviews and removes user access timely.

We discussed these matters with management on August 18, 2023. Management's response to the findings identified in our review is included in the section titled "Agency Response." We did not validate management's response and, accordingly, cannot take a position on whether or not it adequately addresses the issues in this report.

This report is intended for the information and use of management. However, it is a public record and its distribution is not limited.

Sincerely,

Staci A. Henshaw
Auditor of Public Accounts

JDE/clj

Jamestown-Yorktown Foundation

P.O. Box 1607, Williamsburg, Virginia 23187-1607
(757) 253-4838 (757) 253-5299 Fax (757) 253-5110 TDD jyfmuseums.org

December 14, 2023

Staci Henshaw
Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Dear Ms. Henshaw,

Thank you for the opportunity to comment on the Auditor of Public Accounts Results Letter dated September 22, 2023, and emailed to us on November 14, 2023.

The Jamestown-Yorktown Foundation appreciates the efforts of the APA in reviewing and advising the Foundation on the application and management of internal controls. The Foundation will implement process changes to address the findings identified in the review.

Your results letter identified the following (repeat) internal controls areas that we need to address: (1) risk assessments for sensitive systems; (2) audit logging and monitoring controls; (3) appropriate controls to ensure logical access to systems; (4) testing of IT Disaster Recovery Plan; (5) annual security awareness training for information system users; (6) incomplete and outdated policies; (7) some unmet ARMICS requirements; (8) formal policies for the oversight of two current service providers; (9) SOC report for a provider that processes sensitive information; (10) proper evaluation of contracts for leases to comply with GASB 87; and (11) timely removal of administrator-level roles for four HR and Payroll employees.

The Foundation has addressed some of the items listed above, and we are working to address all the remaining items within the next two years. Of note is that the Foundation is on track to hire an Information Security Officer before the end of FY2024. We are hopeful that this position would give focused attention to the Foundation's compliance with internal controls and information security issues.

educating • interpreting • preserving • commemorating

Thank you to you and your staff for your flexibility in completing the fieldwork for this review. Please know that we sincerely appreciate your guidance and support.

Sincerely,

Christy S. Coleman
Executive Director.

CSC/jm

Copy:
The Honorable Thomas K. Norment, Jr.
Dr. Juliet Machie
Jennifer Eggleston, Candice Owens, Scott Reynolds (APA).