REVIEW OF THE

FRONTIER CULTURE MUSEUM

OF VIRGINIA

# NOVEMBER 2020

EXECUTIVE SUMMARY

During calendar year 2020, the Auditor of Public Accounts (APA) conducted two separate reviews of the Frontier Culture Museum of Virginia (Museum): a performance audit of the Museum's information system security controls and an Internal Control Questionnaire review of the Museum's fiscal and administrative processes. Results of these reviews are generally reported in either a comprehensive report or a letter to management, respectively. However, because of the significance of the issues identified during these reviews, this combined special report was prepared.

The purpose of the information system security special project was to review the Museum's information system security policies and procedures, internal controls, and compliance with laws and regulations. The purpose of the Internal Control Questionnaire review was to evaluate if the Museum has developed and implemented adequate internal controls over significant organizational areas and activities. We do not express an opinion on the effectiveness of internal controls as part of this review.

During both reviews, we determined that the Museum does not have sufficient policies and procedures, which are the foundation for the internal control environment. In addition, we determined the Museum is not in compliance with several state requirements. Chart 1 below shows the number of issues identified in each area. The underlying cause of these issues appears to be significant turnover in the last two years.

Number of Issues Identified by Area

Chart 1
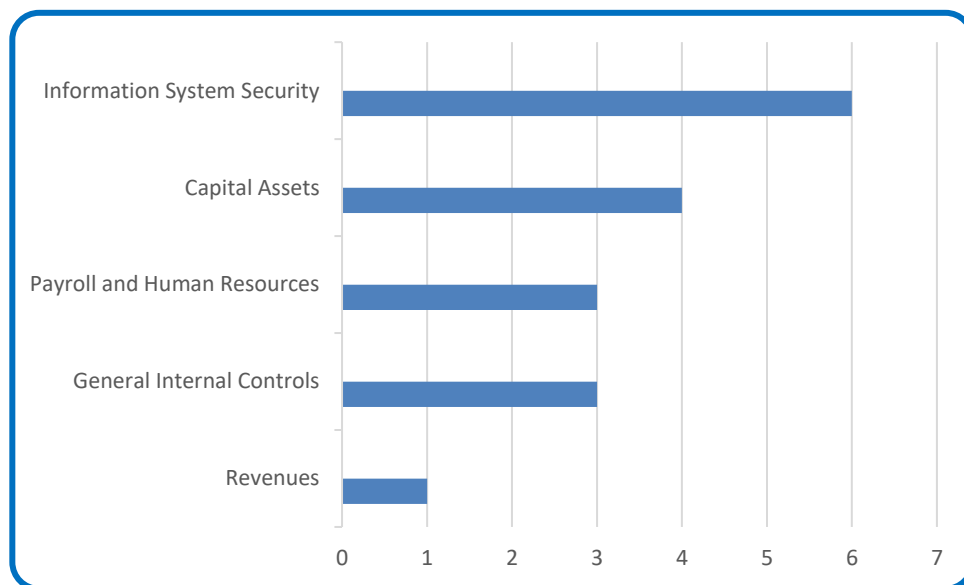
-TABLE OF CONTENTS-

INTRODUCTION

The Auditor of Public Accounts (APA), as required by the Code of Virginia, audits all Executive and Judicial branch Commonwealth agencies handling state funds. However, the Code of Virginia does not require audits of all agencies annually. In order to facilitate a more efficient and effective annual work plan, the APA developed a risk-based approach for auditing agencies that we are not required to audit every year. We refer to these agencies as "cycled agencies." This approach allows the APA the flexibility to focus on the more significant agency operations at any one or several of these cycled agencies. The Frontier Culture Museum of Virginia (Museum) falls into the cycled agency category and is part of this approach.

Under this approach, the APA sends a questionnaire regarding internal controls to the agency at least once every three years to evaluate whether the agency has developed and implemented adequate internal controls over significant organizational areas and activities. We do not express an opinion on the effectiveness of internal controls as part of this review. Agencies are to respond with details of internal controls as of the time they complete the questionnaire. We then review the responses to the questionnaire, and design and perform procedures based on the results. This report reflects our review of internal controls in place at the Museum as of June 2020. It is important to note that we began this review in February of 2020 and, because the most recent full year was fiscal year 2019, most of the transactions we reviewed were from fiscal year 2019.

The APA also performs a separate special project every year that focuses on a single business function that is determined to be significant for the agencies in the cycled agency category. For calendar year 2020, the special project's focus was information system security controls. The purpose of the information system security special project was to review agencies' information system policies and procedures, internal controls and compliance with laws and regulations. We completed a risk analysis to determine which agencies to include in these reviews. The Museum was selected for both reviews.

At the conclusion of the internal control reviews, we generally provide a letter to management stating the results of the review of internal controls and highlighting any key areas of interest. Similarly, at the conclusion of the special project, we provide a comprehensive report detailing the results for the agencies selected for review. However, because of the nature our recommendations for the Museum, this combined special report was prepared.

While there are several factors that led to the findings and recommendations in this report, one of the most significant factors is a lack of policies and procedures combined with a lack of trained and experienced personnel. Policies and procedures are the foundation of the internal control environment and both reviews over the Museum found many critical business areas where there were no policies and procedures. It is especially important to have up to date and thorough policies and procedures during times of significant turnover because institutional knowledge is leaving with the employees who depart.

The Museum did not have a fiscal director for the majority of 2019, the position was vacant from February to early November. In addition, for three months during 2019 (July to September) there were no employees in the fiscal department. The accounting duties during that time were being performed by an employee in a different department who had no accounting education or training and had no experience performing fiscal duties. The Museum has struggled in recent years to fill vacancies in the fiscal department due to several factors including the relatively remote location of the agency, competition with other entities that are able to pay larger salaries, and a general lack of qualified candidates. When the fiscal director began in November of 2019, she was the only employee in the fiscal department until late January and then a little over a month later the COVID-19 pandemic caused the Museum to shut down. The internal control review began just before the shutdown. While the fiscal director did begin to implement changes in the very short time period before the internal control review began, those changes are not reflected in this report since most of the transactions reviewed were from fiscal year 2019.

As shown in Chart 2 below, personal services represents over half of the Museum's annual expenses. Contractual services is also a significant expense for the Museum, representing 37 percent of total expenses. The internal control review focused primarily on internal controls related to these two areas, as well as capital assets, and general internal controls that affect all business processes such as the Museum's documentation of compliance with Department of Account's (Accounts) Agency Risk Management and Internal Control Standards.

Fiscal Year 2019 Expense Breakdown

Chart 2

Other
$344,238
9%

Contractual
Services
$1,367,128
37%

Personal Services
$2,040,405
54%
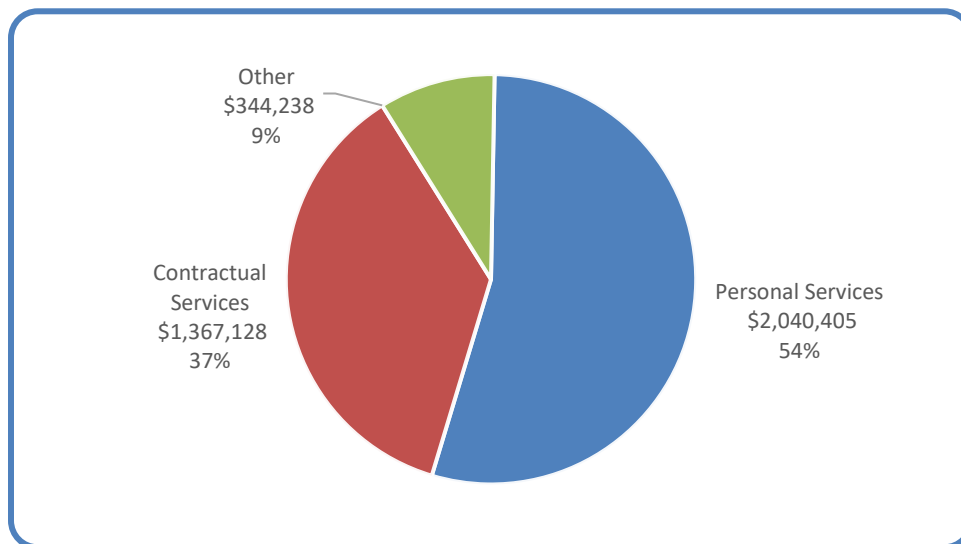
COMMENTS TO MANAGEMENT

Design and Implement Policies and Procedures for all Critical Business Areas

The Museum does not have adequate policies and procedures in place for many of their critical business processes. Instead, the Museum relies on Commonwealth policies and procedures documented in the Commonwealth Accounting Policies and Procedures (CAPP) Manual. CAPP Manual Topic 20905 states the following: "As with every topic in this manual, CAPP Manual procedures alone never eliminate the need and requirement for each agency to publish its own internal policies and procedures documents, approved in writing by agency management. The lack of complete and up-to-date internal policies and procedures, customized to reflect the agency's staffing, organization, and operating procedures, reflects inadequate internal control." We identified a lack of policies and procedures over several fiscal and administrative processes. The following are the areas we identified that management should develop policies and procedures over:

- *Accounting System Reconciliation* – This relates to reconciling agency records with the Commonwealth's accounting and financial reporting system. Management should develop desk procedures to document each step of the reconciliation process.

- *Contract Procurement and Monitoring* – The procedures should cover the contract procurement and management process and how the Museum complies with the Agency Procurement and Surplus Property Manual. The Museum's policy should include procedures to ensure contract administrators sufficiently monitor contract performance and document their monitoring activities. The Museum's policy should also include a provision for the periodic review of procurement and management activities to ensure compliance with state regulations.

- *Financial Reporting* – The procedures should include guidance on how to gather, prepare, review, and verify information submitted to Department of Accounts for inclusion in the Comprehensive Annual Financial Report.

- *Payroll Preparation and Certification* – The procedures should describe how to fulfil the agency responsibilities in the Payroll Service Bureau's Scope of Services document including the pre-certification, certification, and post-certification processes.

- *Snapshot Confirmation* – The procedures should cover how to fulfill the agency's responsibilities of performing retirement benefits system reconciliations prior to snapshot confirmation as stipulated by the Payroll Service Bureau's Scope of Services Document.

- *Collection of Accounts Receivable* – The procedures should include how to verify, track, and collect outstanding accounts receivable.

- *Receipt and Deposit of Funds* – The procedures should include the process by which the Museum receives, safeguards, deposits, records, and reconciles receipts.

- *Capital Asset Management and Inventory* – The procedures should include how to enter, track, depreciate, and dispose of capital assets. In addition, the procedures should include guidance on how to perform a semi-annual inventory in compliance with CAPP Manual requirements. The procedures should also contain guidance to determine whether assets are capitalizable and evaluate their useful lives.

- *Leases* – The procedures should include how to identify, track, and record leases.

- *Capital Outlay* – These procedures should guide the capital outlay process and ensure compliance with CAPP Manual requirements.

- *Small Purchase Charge Card Administration* – These procedures should govern small purchase charge card usage in compliance with topic 20355 of the CAPP Manual.

- *Drawdown of Virginia Public Building Authority Funds* – These procedures should describe the process by which the Museum draws and records Virginia Public Building Authority Funds.

While these were the areas specifically identified during the review, policies and procedures are required for all critical business processes. Management should develop and implement documented policies and procedures for all critical business processes that provide enough detail to allow an individual new to the process to follow them. This will allow operations to continue in the event of turnover and ensure that transactions are processed consistently across the organization. Management should also ensure policies and procedures are reviewed annually or as needed, and that evidence of this review is retained.

Ensure Compliance with the Agency Risk Management and Internal Control Standards

The Museum does not meet the minimum requirements documented in Accounts' Agency Risk Management and Internal Control Standards (ARMICS) standards for agency and transaction-level risk assessments. The Museum was unable to provide any documentation to show compliance with the requirements. The ARMICS process includes, but is not limited to the following:

- creating and actively promoting a Code of Ethics;
- performing an agency-wide risk assessment;
- performing an analysis of strengths, weaknesses, opportunities, and threats;
- identifying, documenting, and testing agency-level controls;
- identifying and documenting significant fiscal processes, which must include financial reporting and reconciliations;
- identifying and documenting the risks to the significant fiscal processes;

- identifying and testing the key controls over each significant fiscal process, including thoroughly documenting tests performed and test results; and
- identifying areas for improvement based on the ARMICS review performed.

The Museum should complete the entire ARMICS process including the agency-level assessment, and the transaction-level assessment, to meet the minimum requirements of CAPP Manual Topic 10305 and the ARMICS Standards. The Museum should ensure that enough documentation is retained to provide evidence of compliance with all parts of the standard.

Perform Reconciliation of Accounting Records

The Museum was unable to provide evidence that it is reconciling internal accounting records to the Commonwealth's accounting and financial reporting system. Management has been certifying monthly to Accounts that the information has been reconciled. Topic 20905 of the CAPP Manual requires the monthly preparation of reconciliations with sufficient detail to assert that all transactions are accurately recorded in the Commonwealth's accounting and financial reporting system. Additionally, agencies are prohibited from submitting month-end or fiscal-year-end certifications until the related reconciliations are complete and fully documented. The Museum should implement and document monthly reconciliations as required by CAPP Manual Topic 20905 prior to submitting certifications to the Department of Accounts.

Comply with State Requirements for Payroll and Human Resource Processes

As noted in Chart 2 above, personal services is the largest expense for the Museum. Although the Museum uses the Department of Account's Payroll Service Bureau (Bureau) to process payroll, the Museum still has a level of responsibility related to payroll and human resources. These responsibilities are outlined in the Bureau's Scope of Services document. By not performing all of its responsibilities, there is an increased risk of employees receiving improper payments, retirement data being incorrect, and errors in the accounting and financial reporting system.

Payroll certification

The Museum does not review data related to wage payments as part of its payroll certification procedures. The Bureau's Scope of Services document requires agencies to, as part of the certification process, review reports for reasonableness with respect to wage payments, salaried overtime payments, new hire payments, terminating employees' final payments and leave payouts, partial salary payments due to absences without leave, and VSDP benefit payments. The Museum should implement and document a review of this data as part of its payroll certification process.

Retirement benefit reconciliation

The Museum does not perform a reconciliation between the human resources system and the Commonwealth's retirement benefits system prior to confirming the accuracy of retirement benefits

data. The Museum also does not perform a review of the cancelled records report. Finally, The Museum does not address items reported on the Virginia Retirement System exception list. The Bureau's Scope of Services document requires agencies to reconcile creditable compensation from the human resources system to a preliminary snapshot in the Commonwealth's retirement benefits system and resolve any differences prior to confirming the snapshot. The Scope of Services document also requires agencies to ensure regular review of the cancelled records report to ensure all information has been recorded correctly; it is the agency's responsibility to ensure retirement benefits system data is accurate. The Museum should ensure that all retirement data is sufficiently reviewed and reconciled before confirming the snapshot.

Payroll expense review

The Museum does not reconcile payroll data from the Commonwealth's payroll system to the Commonwealth's accounting and financial reporting system. The Bureau's Scope of Services document requires agencies to perform, as part of the post-certification process, a reconciliation to ensure expenses were charged to the correct programmatic codes. The Museum should implement and document a post-certification process that meets the requirements described in Payroll Service Bureau's Scope of Services document.

Improve Internal Controls over Assets

We performed a high-level review of internal controls over capital assets and noted the concerns below over several aspects of capital asset management. By not having adequate internal controls over capital assets the Museum is at an increased risk for theft, errors, and misappropriation of assets.

Separation of duties

The Museum does not maintain adequate separation of duties between individuals responsible for maintaining and monitoring physical assets and those responsible for recording fixed assets in the Commonwealth's capital asset system. Topic 30105 of the CAPP Manual requires agencies to establish internal control systems to ensure that physical assets are reasonably protected from theft. Adequate separation of duties is a key control to ensure assets are safeguarded. The Museum should designate an individual with limited or no custody to physical assets as responsible for recording fixed assets in the capital asset system.   If this is not possible, the Museum should implement a managerial review over its physical inventory count process as a mitigating control.

Inventories

The Museum has insufficient documentation of bi-annual inventories. CAPP Manual Topic 30505 requires agencies to conduct a physical inventory of capital assets at least once every two years. The Museum should perform and document bi-annual physical inventories in order to comply with CAPP Manual requirements.

Tracking of leases

The Museum has not implemented a process for tracking its leases and does not enter them into the Commonwealth's lease accounting system. Topic 31215 of the CAPP Manual stipulates all lease agreements should be recorded in the lease accounting system when certain criteria are met. The Museum should track its active leases and record them in the Commonwealth's lease accounting system.

Maintenance reserve

The Museum does not properly track and reconcile maintenance reserve and special project funds. One journal entry tested and one out of twelve expense vouchers tested appeared to record Virginia Public Building Authority (VPBA) related outlays in incorrect fund codes. The Museum should improve its process for tracking, recording, and reconciling VPBA project funds.

Improve Internal Controls over Receipt of Funds

The Museum does not have adequate internal controls in place over the handling of receipts. As noted above, there are no documented policies and procedures over this process, and we noted the following during our review:

- The Museum does not document appropriate separation of duties in its handling of receipts; 100 percent of the deposits reviewed did not include this documentation.

- The Museum was unable to provide documentation for one out of eight deposits requested for testing.

Topic 20205 of the CAPP Manual requires agencies to develop internal processing systems capable of separating receipts from the related accounting processes at the earliest processing point. The Museum should implement and document appropriate separation of duties where funds are handled by agency staff in order to demonstrate its compliance with CAPP Manual requirements. In addition, the Museum should ensure that documents are retained in accordance with the Library of Virginia requirements.

Develop and Implement Policies and Procedures over Information Systems

The Museum does not have policies and procedures over information system security. The Commonwealth's Information Security Standard, SEC 501 (Security Standard), Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, RA-1, SA-1, SC-1, and SI-1 require that agencies maintain policies and procedures over various areas of information system security.

A lack of policies and procedures surrounding information system security may result in insufficient or inappropriate processes and leaves the agency at risk for improper system usage due to lack of formal guidance. The Museum does not have a designated information system security employee

and has never had policies and procedures related to information system security. The Museum should develop and implement policies and procedures surrounding information system security to ensure that the agency's information system processes align with the requirements of the Security Standard.

Improve Access Controls

The Museum does not have adequate access controls in place to ensure that access to their systems is appropriate and complies with the requirements of the Security Standard. Specifically, the Museum has control weaknesses in the following areas:

- The Museum does not have an access control policy in place, as required by Security Standard Section AC-1;

- The Museum does not require a documented request from the user for access to internal information technology (IT) systems, and does not require confirmation of the account request and approval by the IT system user's supervisor and approval by the data owner or designee, or the Information Security Officer to establish accounts on sensitive systems, as required by Security Standard Section AC-2-COV;

- The Museum does not have an adequate process in place for reviewing and confirming ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization, as required by Security Standard Section PS-5; and

- The Museum does not have an adequate process in place for annual review of systems access, as required by Security Standard Section AC-2.

Inadequate access controls could result in improper or unnecessary access to sensitive systems, which could lead to a breach in data security. The Museum has not had an access control policy in place and has not allocated appropriate resources to ensuring access controls are appropriate and the agency's processes are consistent with the requirements of the Security Standard. The Museum should develop and implement access policies, procedures, and processes that align with the Security Standard to ensure consistent and appropriate account management and to ensure the protection of sensitive information.

Develop a Process for Obtaining and Reviewing Audit Logs

The Museum has not implemented some required controls for their third-party service providers, as required by the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard).

The Hosted Environment Security Standard and best practices require and recommend using specific controls to reduce unnecessary risk to data confidentially, integrity, and availability. In general, the Museum does not use three required third-party service provider controls. We communicated these

specific 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 it containing descriptions of security mechanisms.

The Museum should review the third-party service providers reports and ensure the configurations, settings, and controls align with the requirements in the Hosted Environment Security Standard and industry best practices. By not meeting the minimum requirements in the Hosted Environment Security Standard, the Museum cannot ensure the confidentiality, integrity, and availability of data within its systems.

Improve Security Awareness Training Process

The Museum does not have an adequate process in place to ensure that employees complete annual security awareness training. The Museum administers security awareness training during August and September each year, but only 15 out of 36 (42%) salaried employees and 0 out of 7 (0%) sensitive system users completed training between the 2018 and 2019 training cycles. Section AT-2 of the Security Standard requires that the organization provide basic security awareness training to information system users as part of initial training for new users, when required by information system changes, and annually or more often as necessary, thereafter.

If employees do not complete security awareness training, they may not be aware of the Museum and Commonwealth procedures surrounding system security. In addition, security awareness training covers topics that are essential to the protection of the system and Commonwealth data, and a lack of understanding may put information at risk. The Museum has not allocated appropriate resources to information system security, which has resulted in no policies and procedures surrounding security awareness training and an inadequate process of administering and ensuring training is completed. The Museum should develop policies, procedures, and processes to ensure that security awareness training is administered and completed by the appropriate individuals on an annual basis.

Improve and Test Disaster Recovery Plan

The Museum does not have all of the appropriate IT components included in their Disaster Recovery Plan and is not performing an annual exercise of IT Disaster Recovery components. The Museum has identified the systems and Recovery Time Objective (RTO) necessary to recover IT functions, but has not identified a Recovery Point Objective (RPO). Section CP-1-COV-1 of the Security Standard requires that the agency develop IT disaster components of the continuity plan which identifies each IT system necessary to recover agency business functions or dependent business functions and the RTO and RPO for each and that the agency require an annual exercise (or more often as necessary) of IT disaster recovery components to assess their adequacy and effectiveness.

Without a complete and well-tested Disaster Recovery Plan in place, the Museum may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. The Museum has limited IT resources, as the Director of Education performs information technology and security functions in addition to his other duties, which has

resulted in inadequate testing of the plan. The Museum should review and update the Disaster Recovery Plan to ensure that all elements are included and should perform an annual test of IT disaster recovery components to ensure their adequacy and effectiveness.

Improve Oversight of Third-Party Service Providers

The Museum uses third-party service providers (providers) to provide and host two information systems that support their mission-critical business functions. The Museum does not have a process in place to ensure that providers have adequate security controls to protect sensitive data. We identified three weaknesses and communicated them to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to them containing descriptions of security mechanisms.

The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the Security Standard, the Museum cannot ensure the confidentiality, integrity, and availability of data within its systems.

The Museum should dedicate the necessary resources to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard and best practices in a timely manner.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 30, 2020

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
 and Review Commission

   We have performed a review of the Frontier Culture Museum of Virginia and are pleased to submit our report entitled **Review of the Frontier Culture Museum of Virginia**.

   We discussed this report with management on July 2, 2020, and August 26, 2020. Management's response to the findings identified in our review is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

   This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

JDE/vks

COMMONWEALTH OF VIRGINIA

Frontier Culture Museum of Virginia

P.O. BOX 810

STAUNTON, VIRGINIA 24402-0810

Telephone: (540) 332-7850

FAX: (540) 332-9989

November 13, 2020

Martha S. Mavredes, CPA
Auditor of Public Accounts
Commonwealth of Virginia
James Monroe Building
101 North 14th Street, 8th Floor
Richmond, VA 23219

Ms. Mavredes,

    Thank you and your team for conducting your reviews (a performance audit of our IT security controls, and a review of our fiscal and administrative practices), at the Frontier Culture Museum of Virginia. We are very appreciative of the special effort and patience it required to complete the process remotely and under the pandemic constraints we are all managing. We understand that the results of your examination reflect the circumstances in place during the period under review, and may not include information about improvements or changes in practices that we have implemented more recently with the support of new staff at the Agency as well as guidance from DOA, DPB, Payroll Bureau, and Treasury.

    More importantly, we are grateful for the information that this report does include about the areas of operation where we have good opportunities to move forward in our efforts to meet the industry and State standards for best practices and compliance in all matters of internal control. Please thank your team for compiling their combined report in a way that clearly delineates the focus areas we must prioritize. Their commentary and guidance throughout this process have already served as an important resource in our conversations with other State Agencies about strategies we can pursue to meet our mutual objectives (ie options for funding to secure stronger IT infrastructure, negotiations with a POS vendor for a more robust, secure and versatile system, and EWP modifications to ensure clear lines of accountability for tasks which include codification of all policies and procedures).

    We appreciate your work on our behalf, and have a clearer understanding on the paths we need to pursue.

Sincerely,

Megan H. Newman
Executive Director

cc: Jennifer Eggleston APA

"Bringing the Past to Life"
www.frontiermuseum.org

FRONTIER CULTURE MUSEUM OF VIRGINIA
As of June 2020

Megan Newman
Executive Director