DEPARTMENT OF AVIATION

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JULY 2018

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

- TABLE OF CONTENTS -

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 28, 2019

Mark Flynn, Director
Department of Aviation
5702 Gulfstream Rd.
Richmond, VA 23250

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire, completed on July 24, 2018, for the **Department of Aviation** (Aviation). 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 Aviation is responsible for establishing and maintaining an effective control environment.

Review Process

Agencies will undergo an Internal Control Questionnaire review at least once every three years. 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; 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 Aviation. 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

Due to the implementation of the new statewide accounting system, we reviewed system access and 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 each agency. At some agencies only inquiry was necessary; while others included an in-depth analysis of the quality of the Stage 1 Agency-Level Internal Control Assessment Guide, or Stage 2 Process or Transaction-Level Control Assessment ARMICS processes. For Aviation we reviewed all ARMICS documentation.

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: small purchase charge cards, budgeting process, payroll, grants management, and information systems security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are 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:

- Aviation still does not meet the minimum requirements per Accounts' ARMICS standards for agency and transaction-level risk assessments. The Controller and Executive Administrative Manager are working to re-evaluate and improve the agency's ARMICS process. We recommend that they continue focusing on the improvement of this process and use available resources provided by Accounts to ensure the agency is in compliance with applicable standards.

- Aviation is not reporting a loan receivable for bridge loans extended to select grantees with federally eligible projects. The loan amount is typically equal to the state's matching percentage for the grant, and is meant to assist grantees with funding for the beginning stages of the project. Once the recipient receives reimbursement from the federal government, they are required to reimburse Aviation. Management should collaborate with Accounts to determine how to properly report these loans for inclusion in the Commonwealth's Comprehensive Annual Financial Report. Management should also create and implement policies and procedures to document the agency's process of reporting required financial information to Accounts.

- While the Controller and Grants Coordinator have worked together to improve the communication between the Fiscal and Airport Services Divisions, these improvements, to include the reconciliation of grants information per each division's records, are not formalized. Management should continue to reassess the relationship and roles between the two divisions to ensure the Fiscal Division has an active role in monitoring the financial aspects of the various grants and other programs. Management should also ensure the relationship and roles are adequately documented.

- Prior to the appointment of the new Executive Director, Aviation had not developed a detailed budget to adequately monitor the agency's use of Commonwealth funds. During our review, we noted that Aviation was in the process of developing a more detailed budget by division. Management should continue its efforts of developing and managing a more detailed agency budget. Finalizing a detailed budget will help strengthen the agency's process of managing contracts, planning for future projects, succession planning, and other agency initiatives.

- We observed the following information system security related deficiencies:

    - Aviation does not manage website security over the agency website in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) and industry best practices. We addressed these 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. Management should implement controls discussed in the communication marked FOAIE according to best practices and the minimum security requirements in the Security Standard. Doing this will help ensure the confidentiality, integrity, and available of Aviation's sensitive and mission critical data.

    - Aviation has not yet remediated four of the nine findings identified during the three Information Technology (IT) Security Audits completed in January 2016. Additionally, Aviation has not conducted an IT Security Audit of one system requiring an IT security audit within the last three years. Management should mitigate the existing weaknesses identified in the IT security audit findings in order to prevent the risk of malicious parties compromising sensitive and confidential data and mission critical systems being unavailable. Management should complete an IT Security Audit over each sensitive system at least once every three years that tests the effectiveness of controls and compliance with the Security Standard requirements, to help ensure the protection of sensitive and mission critical data.

    - The Aviation IT Risk Management (RM) and Contingency Planning (CP) process and documentation is incomplete and does not include certain attributes needed to effectively evaluate and implement necessary information security controls, including the following items. Aviation is not consistently identifying information systems, including those supporting mission essential functions, and the associated technology versions, among its internal systems list and RM and CP documents. Aviation is not

properly and consistently rating the sensitivity of mission essential systems within its RM and CP documents in accordance with Security Standard. Aviation does not define disaster recovery requirements, including recovery time objectives and recovery point objectives, consistently among its RM and CP documents. Aviation has also not conducted an IT disaster recovery test that includes functional testing, including review and revision of the IT DRP to reflect lessons learned. Aviation should work to address these issues in order to be in compliance with the Security Standard.

We discussed these matters with management on January 9, 2019. 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,

Auditor of Public Accounts

JDE/clj

COMMONWEALTH OF VIRGINIA

Mark K. Flynn
Director

Department of Aviation
5702 Gulfstream Road
Richmond, Virginia 23250-2422

V/TDD – (804) 236-3624
FAX – (804) 236-3635

February 7, 2019

Ms. Martha S. Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

VIA Email: c/o Lauren Griemsman (lauren.griemsman@apa.virginia.gov)
And 1st Class Mail

Dear Ms. Mavredes,

This letter serves as the Department of Aviation's comments on the Internal Control Questionnaire Review Results, dated 28 January 2019. We have reviewed the document and offer the following actions and responses to the findings and recommendations.

We appreciate your department's assistance in understanding and addressing areas of need in the Department of Aviation.

Policies and Procedures – Partial Repeat

We acknowledge the lack of documented policies and procedures for critical administrative functions. We have been working to develop and implement policies and thorough procedures in the areas of human resource management, contract management, revenue billing, and financial reporting. Once policies and procedures are developed, the agency head will review and sign as evidence of approval. As the result of personnel changes in these areas, we have not made as much progress in these areas but are planning to have policies and procedures in place by June 30, 2019.

The Financial Controller is working with the Flight Operations Director to identify the fuel tax spent that requires reimbursement from the IRS using the Redacted. Policies and procedures will be updated by the end of February 2019 to ensure the department's procedure is written.

Agency Risk Management and Internal Control Standards (ARMICS) – Repeat

In previous years, the former Director of Finance and Administration had charged a third-party vendor to complete the ARMICS process. For FY2018, the Director charged DOAV staff to conduct the ARMICS

survey. This process involved surveying all staff as well as involvement from division directors in identifying their critical functions. Once identified, testing of the critical functions was conducted. Our ARMICS report was submitted by the September 30 deadline, however, we were required to submit a Corrective Action Plan for five identified areas, many of which are included in your findings. We have made progress and submitted our 90-day update as of January 15. We expect to have all findings resolved by June 30, 2019.

Reporting Required Financial Information

We are in contact with Department of Accountants (DOA) regarding the recording of bridge loans extended to grantees with federally eligible projects. Currently, the general accounting staff at DOA is looking at the information and will respond back to us with a plan about how we should be handling this potential receivable. Once we hear back from DOA, we will implement a process and develop policies and procedures to document the agency's process of reporting required financial information to DOA.

Reconciliation between Grants and Finance – Partial Repeat

The controller and grants coordinator have worked together to implement a reconciliation process that will ensure the grant information is accurate and reconciliations completed on a monthly basis ensure the integrity of the data. Policies and procedures are being written to document this process and ensure internal controls are in place. This process is expected to be completed by the end of February 2019.

Budgeting Development and Management

DOAV has been working to develop a detailed budget to adequately monitor the agency's use of Commonwealth Funds for FY2019 by agency cost codes. This budget will be given to directors for their review and management use and in compliance with DPB appropriation Redacted system. This February, the department will begin developing a detailed budget for FY2020. The process will ensure the performance budget with DPB and the agency budget in Redacted are in agreement, monitored and provide accurate information in their respective systems. Budgets will be analyzed by the finance department and given to division directors for review. Budget and appropriation adjustments will be made in a timely manner ensuring compliance with all laws and regulations. Director meetings will be held to discuss the budget impact on future projects, succession planning, strategic plans and other initiatives.

Information System Security – Partial Repeat

- Web Application Security

  The agency is in the process of building a new website and estimating going live with this website in the next 60-90 days. As a result of an internal review of existing programs and processes, the website has been classified as non-sensitive by VITA. As a result, audits of the system will no longer be required as there is no sensitive data accessible on the website.

Redacted

Redacted

With the review and reclassification of the existing website and the activation of a new website, the agency is confident that all security requirements will be met.

- Risk Management and Contingency

The former Director of Finance and Administration had charged a third-party IT service provider with conducting the Business Impact Analysis (BIA) for the agency. After an approximately 10-year relationship with the previous IT service provider, the agency severed the relationship and is in the process of reviewing the BIA, which identifies the critical IT systems, the estimated down-time sustainable, and the options for work-arounds in the event of service interruption. In addition, the BIA will be a document more cohesive with the ARMICS and the Continuity of Operations (COOP).

The agency will be working with the new IT service provider to review and revise Risk Management and Contingency Planning processes to address potential risks and incidents.

A desktop exercise involving three occurrences was conducted in November 2018. The third-party vendor conducting the exercise did not consult with DOAV staff to address realistic options involving disaster recovery. The agency will plan to conduct an exercise later this year which will involve realistic IT disaster possibilities and to test the disaster recovery plan in place and make changes where needed.

- IT Security Audit

An audit of the Redacted module was conducted in November-December 2018 by Ernst & Young. The audit resulted in 10 findings, seven of which were issues pertaining to the vendor, GCR. The agency held a teleconference with the vendor and provided a written request outlining the specifications required to be in compliance with sercurity mandates. The agency has requested to receive information on cost and the time frame to implement by February 1, 2019 from the vendor. The remaining findings involved development or strengthening of policies and procedures for end users, which are currently underway.

With regard to the Redacted, this system was terminated as of December 31, 2018 and is no longer in use by the department. This system has not housed social security numbers over the last few years and should not have been deemed a sensitive system or mission critical system as it has been out of commission for the majority of 2018.

We thank you for the time, attention, and detail you have put into this report. We welcome the opportunity to identify and correct the areas of weakness in an effort to strengthen our agency and its programs. While we have made progress in many areas, we understand there is much still to do.

Please let us know if additional information is needed. For Finance-related issues, please contact Roberta Gargiulo at 804-774-4625 or roberta.gargiulo@doav.virginia.gov. For IT-related issues, please contact Laurie Brown at 804-774-4632 or laurie.brown@doav.virginia.gov.

Sincerely,

Mark K. Flynn
Director

100 DOAVAW 20190122 APA Response-Revised