



STATE CORPORATION COMMISSION

AUDIT OF SELECT CYCLES FOR THE YEAR ENDED JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the **State Corporation Commission's (Commission)** contracting and information security cycles for the fiscal year ended June 30, 2019. In addition, we followed up on one procurement finding and two prior information security findings from prior audits. We found:

- proper recording and reporting of related transactions, in all material respects, in the Commonwealth's accounting and reporting system and the Commission's financial system;
- matters involving internal control and its operation necessary to bring to management's attention;
- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and
- adequate corrective action with respect to prior audit findings identified as "Resolved" in the [Findings Summary](#) in the Appendix and satisfactory progress on the finding identified as "Repeat" in the "Status of Prior Year Audit Finding" section of the report.

We did not review management's corrective action on the prior audit finding identified as "Deferred" in the [Findings Summary](#). We will follow up on this finding in a future audit.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
AUDIT FINDINGS AND RECOMMENDATIONS	1-3
AUDIT SCOPE OVERVIEW	4
INDEPENDENT AUDITOR'S REPORT	5-7
APPENDIX – Findings Summary	8
COMMISSION RESPONSE	9-10
COMMISSION OFFICIALS	11

AUDIT FINDINGS AND RECOMMENDATIONS

New Findings

Document Policies and Procedures and Implement Separation of Duties for Legal Service Contracts

Type: Internal Control

Repeat: No

While the Commission has documented its other policies and procedures over procurement and contracting, it has not documented the specific unique procedures it follows for procuring legal services. Additionally, the procedures it follows for obtaining legal services do not incorporate a requirement for more than one person with a working knowledge of the services to be provided to approve in writing the contract, which in the case of legal services is referred to as the letter of engagement. Additionally, the one employee that procures and approves these legal services is the only individual that acknowledges satisfactory receipt of the services for the Commission and approves the payment to the contractor.

Management of the Commission is responsible for establishing and maintaining effective internal controls over procurement and contracting. Documenting policies and procedures aid in communicating expectations and help to maintain a strong control environment. Additionally, separation of duties, the concept of having more than one person required to complete a task, is an internal control intended to prevent fraud and errors.

Without documenting its policies and procedures over procurement and contracting, the Commission may limit its ability to evaluate employees and hold them accountable for deviating from established procedures. Additionally, allowing one employee to initiate and approve a transaction without requiring another individual, with a working knowledge of the situation, to also document their evaluation of the transaction, increases the risk for fraud or an error to occur without detection.

The Commission obtains legal services from a contractor when there is a need for legal services that cannot be adequately fulfilled by its in-house legal counsel or the Virginia Office of the Attorney General. Because these legal services occur infrequently and are procured as needed, the Commission has not dedicated the necessary resources to formalize in writing the specific unique procedures it follows for procuring these services. Additionally, because the Commission and its in-house legal counsel would only agree verbally in meetings as to the precise legal services that were needed, no documentation was generated to provide evidence that others within the Commission agreed that the items in the letter of engagement were reasonable given the facts and circumstances of the situation.

The Commission should formalize and approve in writing the specific unique procedures it follows for procuring legal services. Additionally, the Commission should implement procedures to ensure that separation of duties is developed and documented for evaluating and agreeing to the terms in the letter of engagement and the subsequent payment of invoices for legal services.

Improve Database Security

Type: Internal Control and Compliance

Repeat: No

The Commission does not have certain security controls in place for a mission critical and sensitive system's database in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) and industry best practices, such as the Center for Internet Security's Benchmark.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard requires the implementation of 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 and aligning the database's settings and configurations with best practices, the Commission cannot ensure the confidentiality, integrity, and availability of data within the database or the information it reports.

The Commission should implement the security controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard.

Improve Server Operating System Security

Type: Internal Control and Compliance

Repeat: No

The Commission does not secure the server operating system that supports a mission critical and sensitive system. The Security Standard and industry best practices, such as the Center for Internet Security's Benchmark, require these controls to reduce risk to data confidentiality, integrity, and availability.

We communicated the details of the control weaknesses to the Commission in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to its sensitivity and description of security mechanisms. In general, the critical controls relate to having a baseline configuration that outlines requirements and the minimum configuration settings for server operating systems that store sensitive data, as well as several key settings and controls necessary to secure the system.

The Commission should prioritize and dedicate the necessary resources to address the concerns communicated in the FOIA Exempt document.

Status of Prior Year Audit Finding

Continue Improving Information Security Program

Type: Internal Control and Compliance

Repeat: Partial (first issued in fiscal year 2014, with satisfactory progress in this area)

The Commission is making progress to address an information security weakness communicated in a prior audit report regarding conducting a full revision of its information security program; however, corrective action remains in progress. The Commission has reduced its information security program to 19 core standards and procedures. The Commission has 10 of its 19 standards or procedures in draft form or awaiting approval.

The Security Standard, Section 1.4, requires the Commission to develop and implement an information security program that governs the minimum control requirements for sensitive applications and systems. Without an up-to-date and approved information security program, the Commission may not effectively communicate security requirements to protect data. The Commission also may inconsistently address security needs across the information technology environment, resulting in unauthorized access to data or the inability to recover from system outages promptly.

Turnover within the Commission's Information Security Policy Committee, the departure of the Information Security Officer, and the COVID-19 pandemic resulted in the Commission pausing approval of the standards and procedures in draft form. The Commission plans to complete the information security program update project by June 30, 2021. After completing the information security program update project, the Commission should implement the approved program into its information technology environment. A future audit will include an evaluation of the Commission's completed corrective action and determine whether it satisfactorily resolved the weakness.

AUDIT SCOPE OVERVIEW

The Commission is a constitutionally established independent department of the Commonwealth of Virginia. The Commission is directed by three Commissioners, elected by the General Assembly for six-year terms. The Commission's primary responsibilities include licensing all corporations, limited partnerships, limited liability corporations, and business trusts doing business within the Commonwealth; regulating the utility, railroad, and financial services industries; and adjudicating legal cases brought before it.

Our audit focused on the Commission's contracting, including contract procurement, contract management, contract expenses, and assets resulting from a contract and information security cycles. In addition, we followed up on information security and procurement findings issued in prior audits.

Contracts

Our testing of select contract procurements consisted of emergency, sole source, Quick Quote, and competitive procurements and comparing the Commission's policies and procedures to the related statewide rules. Our testing of contract management included contracts ranging from legal services to information system maintenance. Contractual services are over \$17.5 million of the Commission's expenses, which is roughly 58 percent of non-payroll expenses for the Commission. Our audit also included the testing of the Commission's capitalization of assets resulting from contract expenses to ensure it was consistent with the applicable requirements of set by the Governmental Accounting Standards Board and the Commonwealth Accounting Policies and Procedures Manual.

Information Security

Information systems are critical to the Commission's ability to function; as such, the security of these systems is critical to its ability to carry out its responsibilities. Due to the sensitive nature of this topic, explanations in this report about our information security testing are at a relatively high level.

We assessed the Commission's corrective actions to prior information security and system access findings to determine whether the underlying issues had been resolved. We evaluated the Commission's security controls over one of its databases as well as one of its operating systems. These reviews were based on information security standards promulgated by the Commonwealth and industry best practices.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 4, 2020

The Honorable Ralph S. Northam
Governor of Virginia

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

Commissioners
State Corporation Commission

We have audited the contracting and information security cycles for the year ended June 30, 2019, and followed up on select procurement and information security findings from prior audits for the **State Corporation Commission** (Commission). We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Scope and Objectives

Our audit's primary objectives with regard to the contracting and information security cycles were to review the adequacy of the Commission's internal controls; evaluate the accuracy of resulting expenses related to the contracting cycle and, when applicable, the capitalization of assets in the Commonwealth's accounting and financial reporting system and the Commission's financial system; and test compliance with applicable laws, regulations, contracts, and grant agreements. We also reviewed the Commission's corrective action for select procurement and information security findings from prior reports. We did not review corrective action for the prior audit finding identified as "Deferred" in the [Findings Summary](#) included in the Appendix. We will follow up on this finding in a future audit. See the [Findings Summary](#) included in the Appendix for a listing of all prior findings and the status of follow-up on management's corrective action.

Audit Methodology

The Commission's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, as they relate to the audit objectives, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. We performed audit tests to determine whether the Commission's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the Commission's operations. We performed analytical procedures, including budgetary and trend analyses. We also tested details of transactions to achieve our objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

Conclusions

We found that the Commission properly stated, in all material respects, transactions recorded and reported in the Commonwealth's accounting and financial reporting system and the Commission's financial system, relating to the audit objectives.

We noted certain matters pertaining to the contract procurement and information security cycles, involving internal control and its operation and compliance with applicable laws and regulations that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

The Commission has taken adequate corrective action with respect to select audit findings reported in prior reports that are listed as "Resolved" in the Findings Summary in the Appendix.

Exit Conference and Report Distribution

We provided this report to management on September 15, 2020. Management's response to the findings identified in our audit is included in the section titled "Commission 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, the Commissioners, management, and the citizens of the Commonwealth of Virginia and is a public record.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

GDS/clj

FINDING SUMMARY

Finding	Follow Up Status	Year(s) Issued
Follow Procurement Rules and Best Practices	Resolved	2012 2016
Continue Improving the Information Security Program	Repeat*	2014 2016 2017 2018 2019
Continue Improving Logical Access Controls	Resolved	2016 2017 2018
Develop and Implement Alternative Controls for Manual Payments	Deferred**	2018
Document Policies and Procedures and Separation of Duties for Legal Service Contracts	New	2019
Improve Database Security	New	2019
Improve Server Operating System Security	New	2019

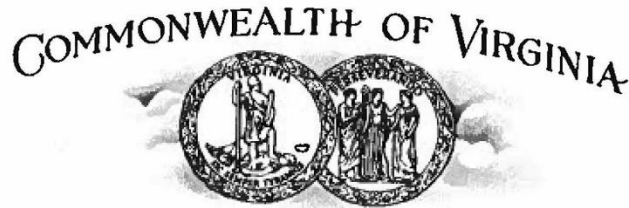
*Follow-up Status on a prior year finding identified as "Repeat" indicates sufficient corrective action on a prior recommendation is not complete; therefore, the prior year finding has been fully or partially repeated.

**Follow-up Status on a prior year finding identified as "Deferred" indicates review of management's corrective action on a prior year finding will be performed in a future audit.

MARK C. CHRISTIE
COMMISSIONER

JEHMAL T. HUDSON
COMMISSIONER

JUDITH WILLIAMS JAGDMANN
COMMISSIONER



STATE CORPORATION COMMISSION

September 23, 2020

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

Dear Ms. Mavredes:

The State Corporation Commission (Commission) appreciates the time and effort your staff devoted to the review of the Commission's contract procurement, management, and expenditures, asset capitalization, and information security for the fiscal year ended June 30, 2019, and the follow-up on one prior procurement finding and two prior information security findings.

We are pleased that your review found that the Commission properly stated, in all material respects, the transactions recorded and reported in our accounting and financial reporting system relating to the audit objectives and adequate corrective action was taken with respect to the prior audit findings of "Follow Procurement Rules and Best Practices", "Continue Improving Logical Access Controls", and satisfactory progress on the prior audit finding of "Continue Improving the Information Security Program".

The Commission will promptly act to resolve the findings for the documenting of policies and procedures and implement separation of duties for legal service contracts, improve database security, improve server operating system security. The following action will be taken regarding the findings.

Document Policies and Procedures and Implement Separation of Duties for Legal Service Contracts

The Commission's practice regarding procuring outside legal services has been intended to preserve important legal privileges and confidentiality. In response to the APA's findings, the Commission will document policies and procedures, to include the separation of duties, for

TYLER BUILDING, 1300 EAST MAIN STREET, RICHMOND, VA 23219-3630 PHONE: (804)371-9608
scc.virginia.gov

procured legal service contracts. The corrective action to implement separation of duties requires, and will be given, careful analysis to prevent potential breaches of necessary legal protections.

Improve Database Security

The Commission's Information Security Officer will work with the appropriate staff to improve database security controls.

Improve Server Operating System Security

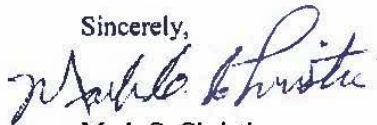
The Commission's Information Security Officer will work with the appropriate staff to improve server operating system security.

Continue Improving Information Security Program

The Commission's Information Security Officer will work with the appropriate staff to continue improving the information security program.

In closing, thank you for the opportunity to review and comment on the audit report. The Commission recognizes the responsibility to implement and maintain internal controls that protect and safeguard Commission resources. We look forward to working with the APA to achieve the shared goal.

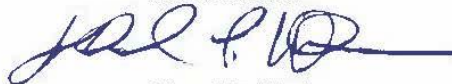
Sincerely,



Mark C. Christie
Chair



Judith Williams Jagdmann
Commissioner



Jehmal T. Hudson
Commissioner

STATE CORPORATION COMMISSION

As of June 30, 2019

Mark C. Christie
Chairman

Judith Williams Jagdmann
Commissioner

Jehmal T. Hudson
Commissioner