



STATE CORPORATION COMMISSION

AUDIT OF INFORMATION SECURITY AND TRAVEL AND SMALL PURCHASE CHARGE CARD EXPENSES FOR THE YEAR ENDED JUNE 30, 2017

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We audited the State Corporation Commission's (Commission) information security and travel and small purchase charge card (charge card) expenses for the fiscal year ended June 30, 2017, including following up on six prior information security findings. We found:

Information Security:

- matters involving internal controls and its operations related to information security necessary to bring to management's attention;
- instances of noncompliance with applicable laws and regulations or other matters related to information security that are required to be reported; and
- adequate corrective action with respect to the prior information security findings listed below.
 - Maintain and Improve Oversight of Third Party Service Providers
 - Retain Evidence of VPN Access Reviews
 - Improve Firewall Security Controls
 - Develop, Implement, and Maintain Information Security Controls

Travel and Charge Card Expenses:

- proper recording of travel and charge card expenses, in all material respects;
- no matters involving internal control and its operation necessary to bring to management's attention; and
- no instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

We did not include the prior audit findings titled "Disable System Access in a Timely Manner" and "Follow Procurement Rules and Best Practices" in the scope of the current audit, but will follow up on these findings in a future audit.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
AUDIT FINDINGS AND RECOMMENDATIONS	1-2
AUDIT SCOPE OVERVIEW	3-4
INDEPENDENT AUDITOR'S REPORT	5-7
AGENCY RESPONSE	8-9
AGENCY OFFICIALS	10

AUDIT FINDINGS AND RECOMMENDATIONS

STATUS OF PRIOR YEAR AUDIT FINDINGS

Continue Improving the Information Security Program

Type: Internal Control and Compliance

Repeat: Yes (first issued in 2014 with significant progress in this area)

The Commission is making progress to address an information security weakness communicated in our previous audit report for not developing and implementing certain information security policies. Since the completion of the last audit, the Commission has developed and implemented a systems interoperability policy and a malicious code protection policy. Additionally, the Commission has drafted policies for systems hardening, system data backup and restoration, and data storage media that are awaiting final approval from the Commission's Information Security Policy Committee. The Commission plans to approve and implement the remaining policies by December 31, 2018. A future audit will evaluate if the Commission's information security policies are working effectively.

Continue Improving Logical Access Controls

Type: Internal Control and Compliance

Repeat: Yes (first issued in 2016, with significant progress in this area)

The Commission is making progress to address an information security weakness communicated in our previous audit report for inadequate logical access controls. Since the last audit, the Commission resolved three of the four weaknesses reported in the prior audit. The Commission has a new process to address the one outstanding item and a future audit will evaluate the process to determine whether the corrective action properly addresses the weakness.

NEW AUDIT FINDING

Improve Database Security Controls

Type: Internal Control and Compliance

Repeat: No

The Commission has not implemented some required security controls in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) and industry best practices, such as the Center for Internet Security, for a database that supports a critical system.

The Security Standard and best practices require and recommend using specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. In general, the Commission does not use two required access management 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 Commission should review the database and ensure the configurations, settings, and controls align with the requirements in the Security Standard and industry best practices. The Commission should also update their database security control processes to align with the Security Standard and best practices. Doing this will help maintain the confidentiality, availability, and integrity of the sensitive and mission critical data stored or processed by the database.

AUDIT SCOPE OVERVIEW

The Commission is a constitutionally established independent agency of the Commonwealth of Virginia. The Commission's primary responsibilities include licensing all corporations doing business within the Commonwealth; regulating the utility, railroad, and financial services industries; and adjudicating legal cases brought before it.

The Commission's most significant cycles are revenues and payroll expenses. These cycles were reviewed during our prior audit, which was for the period July 1, 2014, through January 31, 2016. In addition to those cycles, we also reviewed non-payroll expenses, information security, and various general accounting controls. That audit resulted in seven findings pertaining to information security. Based on the results of the prior audit and the potential risks posed to governmental functions by a lack of information security, we determined that a focused review of the Commission's information security would be included in this audit.

No findings were identified in regards to the Commission's most significant cycles in the prior year; therefore, we also focused the current audit on areas that are traditionally more susceptible to fraud, abuse, and noncompliance, and had not have been reviewed in recent audits. Based on these considerations, we incorporated travel, including travel reimbursements paid to employees, and charge cards into our audit.

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 of our information systems work in this report are discussed at a relatively high level.

We assessed the Commission's response to the information security-related findings from our prior audit to determine whether the underlying issues had been resolved. However, we did not assess the Commission's response to the finding, entitled "Disable System Access in a Timely Manner" because we focused on information security areas we assessed as higher risk. Additionally, we evaluated the Commission's change management process and reviewed the security controls of one of its databases. These reviews were based on information security standards promulgated by the Commonwealth and industry best practices.

Travel Expenses

The Commission incurs significant travel expenses, typically ranking among the highest of non-university Commonwealth agencies. Most of the Commission's travel-related expenses are incurred as reimbursements made to employees; however, the Commission also utilizes the air travel charge card and travel charge card programs offered by the Department of Accounts (Accounts). Air travel charge cards are used exclusively for employee air travel and they are assigned to a limited number of employees. The Commission is responsible for paying the balances on these cards. Travel charge cards are available to Commission employees on an as-needed basis and employees are responsible for paying

the balance on these cards; however, the Commission is liable for the balance in the event that the employee defaults.

We reviewed a sample of travel reimbursements paid during the fiscal year ended June 30, 2017, to ensure that they were reasonable, accurately recorded, and processed in accordance with the Commission's policies and procedures. Additionally, we ensured that none of the selected reimbursements included expenses that had been paid for using agency-sponsored charge cards. We reviewed select air travel charge card transactions to ensure that they were being appropriately used and accurately recorded. We determined that a detailed review of travel charge cards was not warranted after gaining a deeper understanding of the scope of their use within the Commission and re-assessing the risk that their potential misuse could present to the agency and to the Commonwealth. We ensured that both travel-related charge card programs were being administered in accordance with the requirements established by Accounts.

Charge Card Expenses

The Commission participates in the charge card program offered by Accounts. Charge cards are assigned to employees as a means of purchasing various materials, supplies, and services required by their agency to carry out its governmental functions. These charge cards are vulnerable to various forms of misuse in the absence of strong internal controls, as cardholders may seek to purchase personal items using public funds or circumvent traditional procurement-related controls.

We ensured that charge cards were being appropriately used and monitored by the Commission by reviewing relevant policies and procedures to ensure that they were in agreement with Accounts requirements. We ensured that the Commission had an appropriate process in place to assign and monitor the use of the cards by reviewing its process for tracking cardholders and periodically reviewing purchases made with the cards. This was accomplished by reviewing a selection of cardholder reconciliations to verify that they were being appropriately completed and ensuring that all cardholders had been trained regarding acceptable use of the cards. We verified that the internal controls were operating effectively by reviewing selected transactions that presented a higher-than-average chance of constituting breaches in internal control. Such transactions include those that seemed indicative of inappropriate use based on vendor name or the type of items purchased, purchases that may have been placed separately in an effort to avoid transaction limits, and instances in which the Commission may have been erroneously charged twice by a vendor. Additionally, we reviewed instances in which cardholders appeared to have breached their monthly spending limit.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 14, 2018

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

Commissioners
State Corporation Commission

We have audited the information security and travel and small purchase charge card (charge card) expenses at the **State Corporation Commission** (Commission) for the year ended June 30, 2017. 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 was focused on three aspects of the Commission's operations: information security and travel and charge card expenses. Our primary objectives in regards to each are as follows:

- **Information security**: Review of the adequacy of the Commission's information security internal controls, test compliance with applicable laws and regulations, and review the corrective actions taken in regards to certain information security findings from our prior audit.
- **Travel and charge card expenses**: Evaluate the accuracy of transactions recorded, review the adequacy of the Commission's internal controls, and test compliance with applicable laws and regulations.

We did not follow up on corrective actions taken in regards to two findings from our prior audit of the Commission. The finding titled “Disable System Access in a Timely Manner” was issued in relation to the Commission’s internal systems; we decided to focus on information security areas we assessed as higher risk. The finding titled “Follow Procurement Rules and Best Practices,” was issued in relation to the Commission procuring a new system under a single contract, which has been separated into multiple contracts. Management’s corrective actions for these findings will be subject to follow-up procedures in future audits.

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 agreements.

We gained an understanding of 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, placed into operations, and being followed. Our audit also included tests of compliance with provisions of applicable laws and regulations as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents and records, and observation of the Commission’s operations. We performed analytical procedures, including 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 has taken adequate corrective action with respect to four of the six information security findings from the prior audit in which we performed follow-up procedures and that significant progress had been made towards resolving the other two. The information security findings we reviewed and our assessment of the Commission’s corrective actions in regards to those findings are depicted in the table on the following page.

Prior Year Finding	Status
Maintain and Improve Oversight of Third Party Service Providers	Resolved
Continue Improving the Information Security Program	Unresolved, re-issued
Retain Evidence of VPN Access Reviews	Resolved
Improve Firewall Security Controls	Resolved
Improve Logical Access Controls	Unresolved, re-issued
Develop, Implement, and Maintain Information Security Controls	Resolved

In addition, we noted a new matter involving internal control and noncompliance with applicable laws and regulations with regard to the Commission's information security that warrants management's attention and corrective action. Therefore, we have communicated a new recommendation titled "Improve Database Security Controls" in the section entitled "Audit Findings and Recommendations" along with the findings listed in the above table with a status of "Unresolved, re-issued."

We found that the Commission's recording of travel and charge card expenses to be materially correct. We noted no matters involving internal control and its operation pertaining to travel and charge card expenses that we consider necessary to be reported to management. The results of our tests of compliance with applicable laws and regulations, as they pertain to travel and charge card expenses, revealed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

Management's Response and Report Distribution

We provided this report to management on September 17, 2018. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

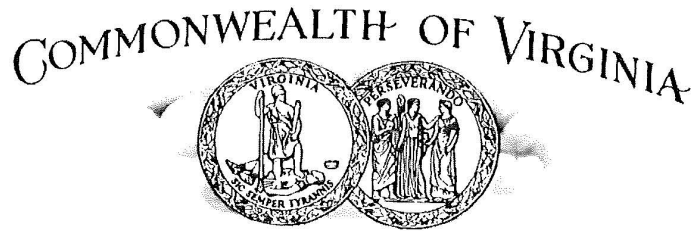
This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

GDS/clj

MARK C. CHRISTIE
COMMISSIONER

JUDITH WILLIAMS JAGDMANN
COMMISSIONER



JOEL H. PECK
CLERK OF THE COMMISSION
P.O. BOX 1197
RICHMOND, VIRGINIA 23218-1197

STATE CORPORATION COMMISSION

September 26, 2018

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 information security program, travel expenses, and use of small purchase charge cards, all for the year ended June 30, 2017.

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, that no matters were noted involving the internal controls pertaining to travel expenses and the use of the small purchase charge cards, and that corrective action was taken regarding four of the six information security findings from the prior audit and that significant progress had been made towards rectifying the other two findings.

The Commission will promptly act to resolve the finding for the database security controls and will continue the action already initiated to correct the two unresolved information security findings from the prior audit. The following action will be taken regarding the other findings.

Implement Database Security Controls

The Commission's Information Security Officer (ISO) will work with the Information Technology staff responsible for the database and assure the security controls required to protect the database are implemented.

Continue Improving the Information Security Program

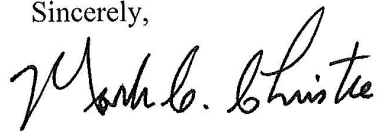
The Commission's Information Security Policy Committee responsible for adopting the policies applicable to the Information Security Program will continue their review of the policies that have been drafted so the policies can be adopted and implemented. The intent is to adopt the policies during fiscal year 2019.

Improve Logical Access Controls

The ISO will work with the appropriate Commission staff and assure the logical access requests for CIS are documented in the Service Desk system.

In closing, thank you for the opportunity to review and comment on the audit report. The Commission recognizes the responsibility to implement and maintain an information security program that protects information resources. We look forward to working with the APA to achieve the shared goal.

Sincerely,



Mark C. Christie
Chairman



Judith Williams Jagdmann
Commissioner

STATE CORPORATION COMMISSION

As of June 30, 2017

Mark C. Christie
Chairman

James C. Dimitri
Commissioner

Judith Williams Jagdmann
Commissioner