VIRGINIA DEPARTMENT OF STATE POLICE

AUDIT OF COMPLETED CORRECTIVE ACTIONS FOR PRIOR AUDIT FINDINGS

FOR THE YEAR ENDED JUNE 30, 2022

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

AUDIT SUMMARY

We audited the adequacy of the Department of State Police's (State Police) corrective actions for the 26 prior audit findings which State Police identified as complete as of June 30, 2022. Specifically, we tested corrective actions within the divisions of: Property and Finance (21); Information Technology (3); and Human Resources (2). Our audit found adequate corrective action for the 26 prior audit findings tested, which we classify as "completed" within the Findings Summary table in the Appendix.

Our audit scope was limited to those areas described above in the first paragraph and in the Audit Scope Overview section. The corrective actions for the 18 prior audit findings not included in the scope of this audit are classified as "ongoing" within the Findings Summary table in the Appendix. We will follow up on these findings in a future audit. However, given the significance of the inherent risks associated with information technology and the controls required by the Commonwealth's Information Security Standard, SEC 501 (Security Standard), we provide status updates on State Police's ongoing corrective actions related to the four findings under the Information Technology division. These updates are within the section titled "Status of Information Technology's Corrective Actions."

-TABLE OF CONTENTS-

AUDIT SCOPE OVERVIEW

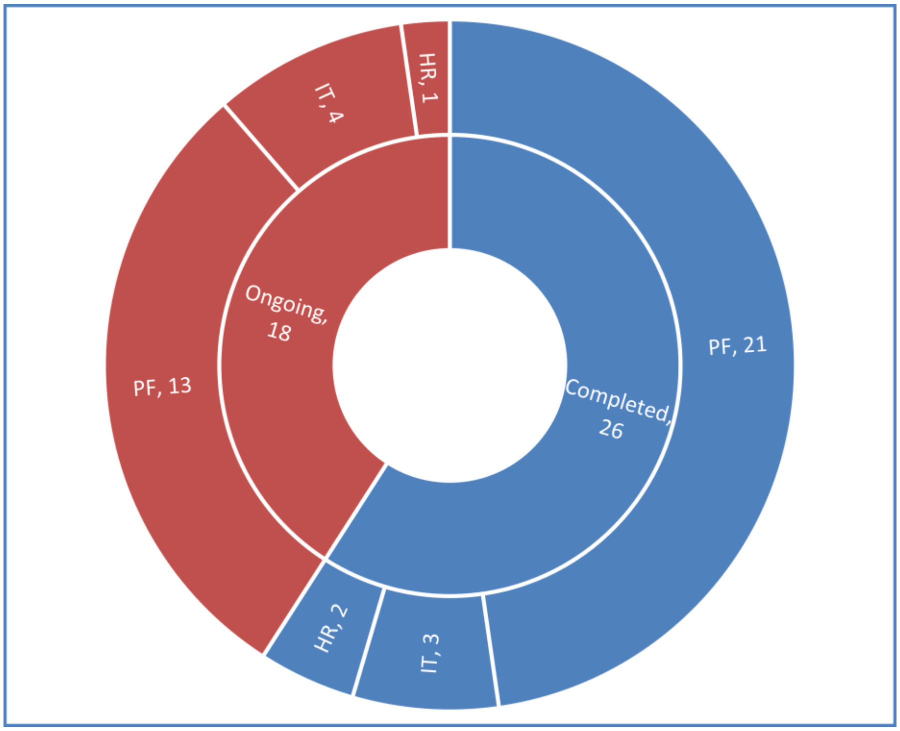
State Police provides services to the public, other law enforcement, and criminal justice agencies. It is organized into three bureaus: the Bureau of Criminal Investigation, the Bureau of Field Operations, and the Bureau of Administrative and Support Services (BASS). BASS consists of several divisions, including Information Technology (IT), Property and Finance (PF), and Human Resources (HR). Below we provide statistics on prior audit findings based on the division responsible for implementing State Police's corrective action.

For our audit of the fiscal year ended June 30, 2022, we tested prior audit findings where State Police indicated they completed its corrective actions. As a result, we performed procedures related to the Human Resource, Information Technology, and Property and Finance divisions. Further, given the significance of the inherent risks associated with information technology and related controls required by the Security Standard, we performed additional procedures to learn the actions that State Police is taking to address four prior information technology findings with ongoing corrective actions to provide a status update, but not for the purpose of evaluating the adequacy of State Police's corrective actions for these findings.

Chart 1 below shows that collectively State Police completed more than half of its corrective actions. The Findings Summary table in the Appendix provides information as to when we first reported each finding to indicate how long corrective actions have been ongoing. The section titled "Status of Information Technology's Corrective Actions" provides status updates on State Police's ongoing corrective actions related to the four remaining findings under the Information Technology division.

Findings Summary

Chart 1



STATUS OF INFORMATION TECHNOLOGY'S CORRECTIVE ACTIONS

State Police's information technology (IT) assets are vital to its mission and include systems that allow law enforcement to effectively coordinate, communicate, and support its financial and administrative operations. State Police has elected to start transitioning its IT assets to be under the purview of the Virginia Information Technologies Agency (VITA) infrastructure environment. However, currently State Police manages its IT assets internally and must adhere to the Commonwealth's Security Standard promulgated by VITA. Our previous audit of State Police's IT controls reported internal control weaknesses and instances of noncompliance relative to the Commonwealth's Security Standard. Below are status updates on State Police's ongoing corrective actions related to the four remaining findings under the division of Information Technology.

Upgrade and Replace End-of-Life Technology

Type: Internal Control and Compliance
First Issued: 2009
Prior Titles: Upgrade Database System Software, 2009 and 2011; Continue to Upgrade Database System Software, 2013; and Continue to Upgrade and Replace End-of-Life Technology, 2017 and 2020

State Police has made some progress upgrading certain technologies since the fiscal year 2020 audit; however, State Police continues to run seven known unsupported technologies that create risk for at least 18 of its applications. Furthermore, State Police does not maintain a current IT system and asset inventory list and as a result, the end-of-life and end-of-support (unsupported) software listed above may not be complete. 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 it containing descriptions of security mechanisms.

The Security Standard requires State Police to prohibit the use of software products that the software publisher has designed as end-of-life/end-of-support. Retired and unsupported software no longer receive updates and patches to remedy recently discovered vulnerabilities. Additionally, the Security Standard requires State Police to document each sensitive system owned by the agency as well as create and periodically review a list of agency hardware and software assets (*Security Standard, Sections 5 Sensitive IT System Inventory and Definition, CM-2-COV Baseline Configuration, SI-2-COV Flaw Remediation*).

State Police has experienced staff turnover since the 2020 fiscal year audit, causing the agency to lack the necessary resources to maintain an IT system and asset inventory list that reflects its current environment. Additionally, State Police delayed its plans to fully transition under the Commonwealth's Information Technology Infrastructure Services Program (ITISP) due to the COVID-19 pandemic and supply chain issues, thus causing State Police to delay upgrading its unsupported technologies.

State Police should obtain the necessary resources to develop and implement the necessary policies, procedures, and security controls to resolve the weaknesses discussed in the FOIAE communication. These actions will help to maintain the confidentiality, integrity, and availability of its sensitive and mission critical data.

Improve Risk Assessments

Type: Internal Control and Compliance
First Issued: 2017

State Police is not regularly updating its sensitive systems listing nor IT risk management documentation for its sensitive systems. Since the fiscal year 2017 audit, State Police contracted with the VITA Shared Information Security Officer Services to complete some of the required IT risk assessments for calendar years 2021 and 2022. However, due to State Police experiencing staff turnover and resource shortages across the agency, including the Information Security Officer position, State Police did not finalize the draft risk assessments it received from VITA. Additionally, State Police is unable to verify which systems require IT risk assessments due to it not updating its sensitive systems list to ensure it is complete.

The Security Standard requires State Police to conduct and document IT risk assessments as needed, but not less than once every three years. Additionally, the Security Standard requires State Police to conduct and document an annual self-assessment to determine the continued validity of the assessments. The Security Standard also requires State Police to document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur (*Security Standard, Sections: 5-Sensitive IT System Inventory and Definition, and 6-Risk Assessment*).

We communicated the control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. State Police should ensure its sensitive systems list is complete and conduct and document the IT risk assessments in accordance with the Security Standard as discussed in the communication marked FOIAE. These actions will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Disaster Recovery Plan

Type: Internal Control and Compliance
First Issued: 2017

State Police continues not to have an updated IT Disaster Recovery Plan (DRP) that reflects its current IT environment. Additionally, State Police continues to not conduct annual DRP tests to ensure it can recover mission critical systems and data according to its Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). State Police has not reviewed nor updated its DRP since 2015 and has not conducted an annual comprehensive test since the last DRP update. We communicated the control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires State Police to develop, maintain, and have the Superintendent approve an IT DRP that supports the restoration of mission essential functions and dependent business functions. The Security Standard also requires State Police to periodically review, reassess, test, and revise the IT DRP to reflect changes in the mission essential functions, services, IT system hardware and software, and personnel (*Security Standard, Section CP1-COV-2 Contingency Planning Policy and Procedures*).

State Police did not make progress with improving its IT DRP because in 2018 it started a project to transition under the purview of VITA's infrastructure environment. As part of this project, State Police planned to update its IT DRP to reflect its new environment. However, State Police and VITA experienced several delays since 2018 that has caused State Police to not complete the transition to VITA. While experiencing project delays, State Police did not update the IT DRP to reflect its current environment due to resource constraints.

State Police should update its IT DPR in accordance with the Security Standard to reflect the current IT environment. State Police should also develop a procedure to perform annual DRP tests against its IT environment to ensure it can recover its sensitive and mission critical systems in accordance with its RTOs and RPOs. This will help to confirm the availability of mission critical applications that State Police relies on to protect the citizens of the Commonwealth.

Improve Backup and Restoration Policies and Procedures

Type: Internal Control and Compliance
First Issued: 2020

State Police resolved two of the three deficient backup and restoration controls identified during our last audit in 2020. However, State Police continues not to maintain current backup and restoration documentation for some of its sensitive systems. Specifically, for the systems selected, State Police does not have updated backup schedules for five of its 29 systems (17%) and could not produce a documented review of backup schedules for eight of ten (80%) vendor hosted systems.

The Security Standard, Section CP-9 Information System Backup, requires that State Police "[c]onducts backups … consistent with recovery time and recovery point objectives" and Section CP-9-COV requires "[a]pproval of backup schedules of a system by the System Owner." These requirements are applicable to State Police and its service providers that host any of its sensitive data.

Outdated or incomplete backup schedules increase the risk that State Police may not be able to restore its sensitive data in accordance with its documented recovery time and recovery point objectives. Furthermore, maintaining updated backup schedules is especially important when an IT environment is transitioning to different platforms as there may become a need to rollback changes to a previously working state.

Three factors contributed to State Police not having updated and complete backup schedules. The first cause is due to the lack of an updated sensitive system inventory listing, which we address in a separate finding. The second cause is due to State Police currently migrating systems to hosted providers, which results in frequent changes in its IT environment. The third cause is the significant staff turnover, including the departure of the Information Security Officer since our last audit.

State Police should prioritize resources to ensure it and its service providers maintain updated backup schedules in accordance with the Security Standard that meet the agency's recovery time and recovery point objectives. This will help maintain the availability of State Police's sensitive systems and information.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 5, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

We have audited the adequacy of the **Department of State Police's** (State Police) corrective actions for prior audit findings which it identified as complete as of June 30, 2022. 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 were to evaluate the adequacy of State Police's internal controls and corrective actions related to prior audit findings which it identified as complete, and test corresponding compliance with applicable laws, regulations, contracts, and grant agreements.

Our review encompassed controls and corrective actions over the following significant cycles, classes of transactions, and account balances.

- Contractual procurement and management
- Employment eligibility
- Federal grant expenses
- Federal indirect cost recoveries
- Information system security
- Prompt pay
- Revenue collections and recording
- Small purchase charge card
- User access

Audit Methodology

State Police'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, 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 State Police'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 State Police's operations. 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 State Police has taken adequate corrective action for prior audit findings relating to the audit objective that are listed as completed in the Findings Summary in the Appendix.

We found that State Police is still in the process of taking corrective action for certain matters pertaining to information technology, involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements as described in the section titled "Status of Information Technology's Corrective Actions."

Exit Conference and Report Distribution

We discussed this report with management on December 19, 2023. 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.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

GDS/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Information Technology		
Upgrade and Replace End-of-Life Technology	Ongoing*	2009
Improve Risk Assessments	Ongoing*	2017
Improve Disaster Recovery Plan	Ongoing*	2017
Improve Backup and Restoration Policies and Procedures	Ongoing*	2020
Align Information Technology Security Audits with Current Sensitive Systems	Completed	2017
Perform Information Technology Security Audits	Completed	2017
Obtain, Review, and Document Service Organization Control Reports of Third-Party Service Providers	Completed	2017
Property and Finance		
Align Capital Asset Accounting Policies with Code of Virginia and CAPP Manual	Ongoing	2013
Complete Capital Asset Physical Inventories in Accordance with CAPP Manual Guidelines	Ongoing	2013
Update the Commonwealth's Capital Assets System to Reflect Asset Disposals	Ongoing	2013
Strengthen User Access Policies and Procedures	Ongoing	2013
Improve Processes over Work Zone Project Billings	Ongoing	2013
Align Internal Policies and Procedures with the Virginia Debt Collection Act and Commonwealth Accounting Policies and Procedures	Ongoing	2017
Improve Accounts Receivable Collection Process	Ongoing	2017
Improve Accounts Receivable Tracking Process	Ongoing	2017
Ensure Reconciliation Policies and Procedures Meet CAPP Manual Requirements	Ongoing	2017
Enter Assets into the Commonwealth's Capital Asset System in a Timely Manner	Ongoing	2017
Document Internal Policies and Procedures	Ongoing	2018
Create and Implement Internal Controls over Reconciliations	Ongoing	2018
Maintain and Reconcile a Construction in Progress Schedule in Accordance with CAPP Manual Requirements	Ongoing	2020
Perform Purchase Card Program Administrator Responsibilities	Completed	2013
Align Internal Purchase Card Policies with CAPP Manual Best Practices	Completed	2017
Complete Cardholder and Supervisor Training Annually	Completed	2017

Finding Title	Status of Corrective Action	First Issued
Complete Purchase Card Reconciliations Timely	Completed	2017
Retain Adequate Documentation to Support Purchase Card Program	Completed	2017
Publish Updated Internal Procurement Policies and Procedures Manual	Completed	2017
Perform Contract Management Responsibilities	Completed	2017
Improve Documentation of Sole Source Contract Procurements	Completed	2017
Deactivate Access to the Commonwealth's Purchasing System	Completed	2017
Ensure Timely Removal of Terminated Employee Access	Completed	2017
Submit Indirect Cost Rate Proposals Timely	Completed	2017
Designate Contract Administrator and their Responsibilities in Writing	Completed	2018
Document Contractor Payment Tracking and Performance Evaluations	Completed	2018
Establish and Maintain a Term Contract Listing	Completed	2018
Evaluate and Document Revenue Processes	Completed	2018
Evaluate Fees and Revenues to Ensure Proper Account Coding	Completed	2018
Implement Segregation of Duties over Deposit Processes	Completed	2018
Process and Record Deposits Timely	Completed	2018
Improve Internal Controls over Grant Expenditures	Completed	2018
Improve Monthly Certification over Grant Expenditures	Completed	2018
Ensure Compliance with Prompt Pay	Completed	2018
Human Resources		
Document Retirement Benefits System Reconciliations	Ongoing	2017
Comply with Employment Eligibility Requirements	Completed	2020
Improve User Access Controls to the Retirement Benefits System	Completed	2020

*Given the significance of the inherent risks associated with information technology and the controls required by the Security Standard, we provide status updates on State Police's ongoing corrective actions related to the four findings under the division of Information Technology. These updates are within the section titled "Status of Information Technology's Corrective Actions."

Status of Corrective Action identified as "Ongoing" in the above table reflects the 18 prior audit findings not included in the scope of this audit which we will follow up on in a future audit.

COMMONWEALTH OF VIRGINIA

Colonel Gary T. Settle
Superintendent
(804) 674-2000

DEPARTMENT OF STATE POLICE
P. O. Box 27472, Richmond, VA 23261-7472

Lt. Colonel Kirk S. Marlowe
Deputy Superintendent

December 5, 2023

Ms. Staci Henshaw, CPA
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

We appreciate the opportunity to review the 2022 Virginia State Police Audit Report. Thank you for the recommendations on our information technology control operations, as well as the professionalism of your staff throughout the engagement. We have discussed with your staff the specific items mentioned in the report throughout the course of your review.

We will prepare a formal Corrective Action Plan to address the report findings as required by the CAPP Manual Topic 10205. We will track the progress through completion of the internal desk procedures and auditable documentation to strengthen the internal controls safeguarding Commonwealth assets. We are committed to ensuring the full implementation of the recommendations documented in the report in a timely manner.

We give your comments the highest level of consideration as we continue to improve our practices and compliance with the Commonwealth's policies, regulations, laws, and security standards. We remain committed to focusing staff and resources prudently as we execute the Department's Public Safety mission.

Sincerely,

Gary T. Settle

Superintendent

GTS/DMM

VIRGINIA DEPARTMENT OF STATE POLICE

As of June 30, 2022

Terrance C. Cole
Secretary of Public Safety and Homeland Security

Colonel Gary T. Settle
Superintendent

Lieutenant Colonel Tracy S. Russillo
Deputy Superintendent

Colonel Tricia Powers
Director of Bureau of Administrative and Support Services

Captain Chad Rogers
Information Technology Division Commander

Captain Marilyne Wilson
Property and Finance Division Commander

Captain Jeremy Kaplan
Human Resources Division Commander