



ALCOHOLIC BEVERAGE CONTROL AUTHORITY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov
(804) 225-3350



AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Alcoholic Beverage Control Authority (Authority) as of and for the year ended June 30, 2024, and issued our report thereon, dated December 7, 2024. Our report, included in the Authority's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the Authority's website at www.abc.virginia.gov. Our audit found:

- the financial statements are presented fairly, in all material respects;
- five internal control findings requiring management's attention; however, we do not consider them to be material weaknesses;
- four instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- corrective action on prior audit findings remains ongoing as indicated in the Findings Summary included in the Appendix.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-7

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

8-10

AUTHORITY RESPONSE

11-13

APPENDIX – FINDINGS SUMMARY

14

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Internal Controls Over Employee Separation Process

Type: Internal Control

Severity: Significant Deficiency

First Reported: Fiscal Year 2022

The Alcoholic Beverage Control Authority (Authority) does not have adequate internal controls over the completion of employee separation checklists or removal of systems access for terminated employees. During our review, we found the following deficiencies:

- For four out of 22 (18%) terminated employees, there were variances ranging from 15 days to 11 months between the termination date in the Commonwealth's human resource and payroll system and the termination date on the terminated employees' personnel files;
- For nine out of 23 (39%) terminated employees, the Authority did not enter the termination date timely in the Commonwealth's human resource and payroll system;
- For four out of 11 (36%) terminated employees, the employee separation checklist did not indicate a timely return of Authority property; and
- For ten out of 23 (43%) terminated employees, the Authority did not remove system access timely.

The Authority's Employee Separation Policy (Policy) states, "Supervisors will initiate a Payroll Action Notice (PAN) and separation checklist process on the same workday the employee is separated from the Authority, after the employee has left the premises. The standard time for Division Directors to complete the Employee Separation Checklist is 5 business days after the effective date of separation." The Authority's Policy also states, "In cases of voluntary separation, each Division Director, in conjunction with the Director of Human Resource and CEO, may initiate immediate termination or restriction of an employee's computer access to Authority systems upon initial notification of an employee's intended separation date." By not timely initiating and submitting PANs, which notifies the Authority's Human Resource Department to update employment information after termination, as well as completing employee separation checklists timely, the Authority risks terminated employees receiving incorrect payments, not returning Authority property, and retaining unauthorized access to critical systems.

The Authority should review and update their current termination policies and procedures to ensure adequate and effective internal controls are in place. The update should include adding a requirement in the Policy to disable systems access within a defined time period. Additionally, due to the Authority's unique structure, the Authority should define specific procedures for retail store employees, enforcement employees, and headquarter employees as access levels and risks are inherently different. These enhancements will enable Human Resources to better monitor and hold

supervisors accountable for the timely notification of employee separations, completion of employee checklists, and removal of systems access.

Improve IT Risk Management and Contingency Planning

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Reported: Fiscal Year 2023

The Authority continues to not manage its information technology (IT) risk management and contingency planning program in accordance with its Information Security Risk Management Policy (Risk Management Policy), its Information Security Policy (Security Policy), its Information Classification Policy (Classification Policy), and its adopted information security standard, the National Institute of Standards and Technology Standard, 800-53 (NIST Standard). The following weaknesses continue to exist:

- The Authority does not update its IT System and Data Sensitivity Classifications (Data Sensitivity Classification) as part of its Business Impact Analysis (BIA) process. While the Authority updated its BIA in June 2023, the Authority experienced staff turnover and therefore conducted a new BIA survey process during fiscal year 2024 and is still in process of verifying responses, causing delays in completing the Data Sensitivity Classification. This has also led to the Authority not having a current and accurate system inventory. The Security Policy requires the Authority to review the BIA annually, or more often as necessary, to ensure it is current, accurate, and complete. Additionally, the Classification Policy requires the Authority to identify, classify, and protect IT systems and information that includes a sensitivity ranking for confidentiality, integrity, and availability. The NIST Standard requires the Authority to develop and update an inventory of organizational systems at an organizationally defined frequency. By not having an updated Data Sensitivity Classification that categorizes systems based on confidentiality, integrity, and availability of the data, the Authority increases the risk of inaccurate system classification. This could potentially lead to the Authority not implementing necessary security controls for its systems and IT environment to align with the BIA (*Classification Policy, section: Purpose of Policy, Security Policy, section: 3.3.5.3.1.a IT Contingency Planning; NIST Standard, sections: RA-2 Security Categorization, PM-5 System Inventory*).
- The Authority does not have a completed risk assessment on record for 14 of its 16 (88%) sensitive systems. Additionally, of the two documented risk assessments, the Authority has not conducted an annual review for either. The Authority's Risk Management Policy requires the Authority to conduct a risk assessment for critical information systems and critical production applications at least once every three years. Additionally, the Risk Management Policy requires the Authority to conduct a risk assessment of the potential security-related impacts whenever the Authority stores or processes sensitive information in computer systems. The Security Policy requires formal risk assessments of sensitive systems every three years, with informal risk assessments in other years. Without completing risk assessments

for each sensitive system at least once every three years, the Authority may not identify potential risks in their sensitive systems, which increases the risk of not having mitigating controls in place to prevent a compromise of its sensitive data (*Risk Management Policy, section: 2.c Information System Security Risk Assessment; Security Policy, section: 2.2.3 Infosec Program Activities Inputs and Outputs; NIST Standard, section: RA-3 Risk Assessment*).

- The Authority does not have a complete System Security Plan (SSP) for any of its 16 sensitive systems. The Security Policy requires the Authority to complete a SSP for all sensitive IT systems and perform an annual review for updates. Not having a SSP for each sensitive system could result in the Authority not properly identifying and mitigating risks, which could result in weaknesses exploited by bad actors and potentially compromise the Authority's sensitive information (*Security Policy, section: 3.3.10.3.2.a Application/System Development Life Cycle Security NIST Standard, section: PL-2 System Security and Privacy Plans*).
- The Authority does not test its Continuity of Operations Plan (COOP) in accordance with its testing strategy. The Authority last performed an annual COOP training exercise and test in calendar year 2020 with plans to perform another test in August 2024, which falls outside of the fiscal year audited. The Authority's COOP requires it to conduct annual exercises, which may include tabletop, functional, full-scale, or evaluation exercises. The NIST Standard requires the Authority to test the contingency plan to determine the effectiveness of the plan and readiness to execute the plan, review the contingency plan test results, and initiate corrective actions, if needed. Not regularly testing the COOP could result in the Authority's inability to execute the COOP successfully when needed to support the contingency procedures and ensure IT resources are operational (*NIST Standard, section CP-4 Contingency Plan Testing; Continuity Plan, section: Training and Exercises*).
- While the Authority documented a strategy for disaster recovery training and executed a tabletop exercise in June 2024, the Authority's strategy does not include a full system recovery as part of the disaster recovery test. The Authority's IT Disaster Recovery Plan (IT DRP) requires the Authority's IT Services Division (ITSD) to document tests and lessons learned quarterly. The NIST Standard requires the Authority to test the effectiveness of incident response capabilities for systems and coordinating incident response testing with elements responsible for related plans, such as the COOP and IT DRP. Additionally, the NIST Standard requires the Authority to conduct a full recovery and ensure a reconstitution of a system to a known state occurs as part of contingency plan testing. By not conducting a full system recovery test as part of its IT DRP testing, the Authority may experience significant delays restoring critical IT systems in the event of an emergency due to staff not being adequately prepared (*IT DRP, section: Backup, Recovery, and Testing Strategy; NIST Standard, sections: IR-3 Incident Response Testing, CP-4 Contingency Plan Testing, CP-9 CE2 System Backup: Test Restoration Using Sampling*).

The Authority experienced significant turnover in upper management and the IT department, causing the Authority to pause its corrective actions. Additionally, the delays in completing a BIA and Data Sensitivity Classification led to the Authority not having an accurate system inventory and complete risk management documentation.

The Authority should dedicate the necessary resources to complete its review and revision to its Data Sensitivity Classification as part of the BIA process to ensure its systems' sensitivity classification is accurate. The Authority should conduct risk assessments and develop SSPs for its systems it deems sensitive. Additionally, the Authority should perform annual reviews of the Data Sensitivity Classification, the risk assessments, and the SSPs to ensure that they are relevant and up to date. The Authority should revise its disaster recovery strategy to include a full system recovery and execute its COOP and DRP testing strategies as defined to ensure it can restore critical system functionality within the defined recovery timeframe in the event of a disaster. These actions will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission-critical systems and data.

Ensure Follow-Up Inventories are Performed

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Retail Operations department did not ensure district managers performed a second inventory count for 12 out of 14 stores (86%) where actual inventory on hand was less than the amount recorded within the inventory control system. Furthermore, the Retail Operations Department did not retain records of the actual physical inventory counts for two out of 40 stores (5%).

The Authority's inventory policy requires an annual physical inventory count for each store, which includes documentation, as well as an exception report for differences between the actual inventory and the amount recorded in the Authority's inventory control system. Per the Authority's policies and procedures, the Authority should schedule a second inventory for the store(s) within the same fiscal year if the results of a physical inventory count show a variance equal to or exceeding 0.15 percent. The Virginia Public Records Act (§ 42.1-85 of the Code of Virginia) requires each agency to ensure that it preserves, maintains, and makes accessible public records throughout their lifecycle. Further the Library of Virginia's general schedule number GS-102 requires inventory control system records to be retained for three years after the end of the state fiscal year. Without reperforming physical inventory counts and properly maintaining physical inventory count documentation, the Authority cannot ensure complete physical inventories have occurred, have difficulty investigating discrepancies, and risks reporting the incorrect dollar amount of store inventory.

Due to turnover occurring at the Authority during the fiscal year in district manager positions, and confusion regarding which district manager was responsible for each store, the Retail Operations department provided inconsistent directions to district managers regarding follow-up inventories and, therefore, the stores did not perform required follow-up inventories. The Retail Operations department should ensure district managers are aware of the stores for which they are responsible, communicate to

district managers the requirement for follow-up inventory counts, when necessary, and ensure completion of follow-up inventory counts. Lastly, the Retail Operations department should ensure stores retain inventory documentation in compliance with the Code of Virginia and Library of Virginia requirements.

Improve Physical and Environmental Security Policy and Processes

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Authority does not require and has not implemented certain physical and environmental security requirements in accordance with the NIST Standard. We identified five control weaknesses and communicated them 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 NIST Standard requires the Authority to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the Authority's IT mission-critical systems and data.

The Authority has experienced significant staff turnover in the past year, resulting in staffing constraints that led to the five weaknesses. In addition, the Authority's inconsistent and incomplete risk assessment process, as communicated to the Authority in the audit finding titled "Improve IT Risk Management and Contingency Planning Program" contributed to the identified weaknesses concerning physical and environmental security. Finally, the lack of policy reviews and revisions led to the absence of defined controls and processes within the Authority's policy as required by the NIST Standard.

The Authority should obtain and dedicate the necessary resources to ensure that its physical and environmental security policies and procedures align with the NIST Standard requirements. The Authority should also implement the controls required to address the weaknesses identified in the FOIAE communication, which will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission-critical systems and data.

Continue Improving Oversight of Third-Party Service Providers

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Reported: Fiscal Year 2020

The Authority has made limited progress since the prior year to develop a formal and consistent process to oversee and manage its IT third-party service providers (providers) in accordance with the NIST Standard. Providers are entities that perform tasks and business functions on behalf of the Authority.

Since the prior year's audit, the Authority updated its IT SOC Review Procedure (SOC Review Procedure) to require the Information Security department or functional area responsible to annually

review a System and Organization Controls (SOC) report for each provider classified as sensitive. However, as follows two prior weaknesses continued to exist and we identified one new weakness:

- The Authority's SOC Review Procedure does not accurately reflect the current process used to maintain oversight over the Authority's providers. The SOC Review Procedure requires the Authority to receive and review a SOC report for only those providers classified as sensitive annually. However, the Authority's SOC review process currently is to request and review SOC reports for all providers, no matter the sensitivity classification, and does not define the expected process for providers that the Authority has not classified as sensitive. Additionally, the Authority does not define in its SOC Review Procedure its expectations for gaining other forms of assurance if the Authority cannot obtain a SOC report from a provider. The NIST Standard requires the Authority to employ organizationally defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. By not having a policy or procedure that establishes requirements for monitoring control compliance of all providers on an ongoing basis, the Authority cannot validate that the providers have effective IT controls to protect the Authority's sensitive and confidential data, increasing the chance of a breach or possible data disclosure (NIST Standard, section: SA-9 External System Services).
- The Authority has not completed a formal risk assessment for 32 of its 40 (80%) providers. The Authority's IT Risk Management Policy requires that the Information Security department perform a risk assessment for all new, replacement, and production systems, and to conduct risk assessments for critical information systems and production applications at least once every three years. Without completing risk assessments, the Information Security department is unable to determine the risks that impact its sensitive data or providers and dedicate the resources to ensure the appropriate implementation of security controls to reduce or mitigate those risks (IT Risk Management Policy, section D.2.a Information Security IT Risk Assessment, Evaluation and Report; NIST Standard, section: RA-3 Risk Assessment).
- The Authority has not received and reviewed independent audit assurance that provides an opinion over the operating effectiveness of the controls in place for nine of its 40 (23%) providers. The NIST Standard requires the Authority to employ organizationally defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. By not receiving and reviewing independent audit assurance, such as a SOC report, for each provider on an ongoing basis, the Authority cannot validate that the providers have effective IT controls to protect the Authority's sensitive and confidential data, increasing the chance of a breach or possible data disclosure (NIST Standard, section SA-9 External System Services).

Due to significant turnover in upper management and other staffing constraints, the Authority did not have adequate resources and was unable to make progress to complete formal risk assessments. Additionally, the absence of a SOC Review Procedure that accurately reflects the Authority's current and

expected process, as well as the lack of completed risk assessments, led to the Authority not obtaining and reviewing the independent audit assurance necessary to validate the implementation of security controls.

The Authority should revise its policy and procedure to require and reflect the process the Authority uses to monitor control compliance of all providers at regular intervals, such as obtaining and reviewing independent audit assurance for each provider on an annual basis. As part of the revision, the Authority should ensure the policy and procedure reflects the Authority's process for gaining assurance if the provider does not provide an independent audit assurance report. The Authority should also conduct a formal risk assessment for each provider to determine the potential risks that may impact the provider, the security controls necessary to mitigate the risks, and determine the sensitivity of the data handled by the providers. Finally, the Authority should validate that management implements effective IT controls as required to mitigate potential risks by obtaining and reviewing independent audit assurance, such as a SOC report. These actions will help to safeguard the confidentiality, integrity, and availability of the Authority's sensitive and mission critical data.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 7, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Virginia Alcoholic Beverage Control Authority Board of Directors
Virginia Alcoholic Beverage Control Authority

Dale Farino
CEO, Virginia Alcoholic Beverage Control Authority

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Virginia Alcoholic Beverage Control Authority** (Authority) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated December 7, 2024.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Internal Controls over Employee Separation Process," "Improve IT Risk Management and Contingency Planning," "Ensure Follow-Up Inventories are Performed," "Improve Physical and Environmental Security Policy and Processes," and "Continue Improving Oversight of Third-Party Service Providers," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that is required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings titled "Improve IT Risk Management and Contingency Planning," "Ensure Follow-Up Inventories are Performed," "Improve Physical and Environmental Security Policy and Processes," and "Continue Improving Oversight of Third-Party Service Providers."

The Authority's Response to Findings

We discussed this report with management at an exit conference held on December 9, 2024. Government Auditing Standards require the auditor to perform limited procedures on the Authority's response to the findings identified in our audit, which is included in the accompanying section titled "Authority Response." Certain information, marked with a black box, was redacted from the response as the information is Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Authority's response was not subjected to the

other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the prior reported findings identified as ongoing in the [Findings Summary](#) included in the Appendix.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

AVC/vks

Virginia Alcoholic Beverage Control Authority

Chief Executive Officer
Dale F. Farino



Chair
Timothy D. Hugo
Vice Chair
L. Mark Stepanian
Board of Directors
William D. Euille
Gregory F. Holland
Lisa N. Jennings

December 7, 2024

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
101 N. 14th Street
Richmond, VA 23219

Dear Ms. Henshaw,

Attached are the Virginia Alcohol Beverage Control Authority ("VA ABC," the "Authority") responses to the audit findings for fiscal year ended June 30, 2024. The Authority appreciates the opportunity to respond to the findings noted, and to strengthen our controls based on the recommendations. Our responses to the findings in the Report on Internal Controls are as follows:

Improve Internal Controls over Employee Separation Process

VA ABC concurs with the audit finding. The Authority will reassess its current termination policies and procedures to ensure that adequate and effective internal controls are in place, including a requirement in the policy to disable system access within an organization-defined time period. Furthermore, the Authority will provide additional training and support to the responsible leaders in our retail store division, enforcement division, and headquarters and will conduct quarterly audits to ensure compliance. Human Resources will coordinate with the Authority's Internal Audit division to review the separation checklist items to determine and define the risk associated with each one.

Improve IT Risk Management and Contingency Planning

VA ABC concurs with the audit finding. The Information Security team is working with system owners within the Authority to review, document, and complete the Business Impact Analysis (BIA) to include data sensitivity classifications. While the Authority has prioritized the review of its more sensitive systems, the team is working through its risk assessments to identify potential security-related impacts when sensitive information is stored or processed in VA ABC's computer systems, and to develop a system security plan (SSP) for each.

VA ABC Bureau of Law Enforcement (BLE) partially concurs with the audit finding of testing its Continuity of Operations Plan (COOP). The COOP was actively deployed during the COVID emergency period and did not require testing from 2020 to 2023. The Governor lifted the state-wide "State of



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

Emergency” on June 30, 2021. The Virginia Department of Public Health maintained their declared “Public Health Emergency” until May 12, 2023. Virginia ABC maintained a modified level of COOP operations as most of the ABC workforce was still teleworking or had adjusted work hours. Shortly after the end of the health emergency, ABC began the planning process to update and reinstate the COOP testing.

The Essential Records and IT Function section of the VA ABC COOP was tested by Information Security and Security Operations as part of a series of cyber security testing with VITA. Additional testing of the COOP was conducted to test the emergency call back process of the plan.

VA ABC’s Information Technology Disaster Recovery testing plan documents real-world events and tabletop exercises. This activity lines up with the base National Institute of Standards and Technology Standard, 800-53 (NIST Standard). We do not plan to use control enhancements in this area.

Ensure Follow-Up Inventories are Performed

VA ABC concurs with the audit finding. The Authority has established and updated standard operating procedures and controls in place over retail inventory counts (SOP), but due to the turnovers that occurred at the Authority during the current fiscal year, there were inconsistencies in implementing the Authority’s SOP at the stores. Retail’s upper management is aware of the inconsistencies and has plans in place to re-train store personnel. The Director of Retail Operations will have monthly meetings with the district managers to ensure SOPs over inventory count are done properly. In addition, the Director of Retail Operations has collaborated with VA ABC’s Internal Audit division to ensure that follow-up procedures are done in accordance with the Authority’s SOP.

The Authority’s SOP has defined the leadership owners over who should ensure that physical inventory count follow-ups are scheduled for stores that meet or exceed the defined variance thresholds. Retail’s upper management will monitor and ensure that defined owners of physical count inventory are implementing the SOPs properly and timely.

Lastly, the Authority ensures that inventory documentation is retained in compliance with the Code of Virginia and Library of Virginia requirements, wherein GS-102 requires inventory control system records to be retained for 3 years after the end of the state fiscal year. The Authority’s Inventory Reports, the inventory results by store, and all corresponding inventory adjustments are retained electronically for the required 3-year period and may be retrieved from the Data Warehouse at any time.

Improve Physical and Environmental Security Policy and Processes

VA ABC concurs with the audit finding.

[REDACTED]

[REDACTED]

VA ABC will review and update the Physical and Environmental Security Policy.

[REDACTED]



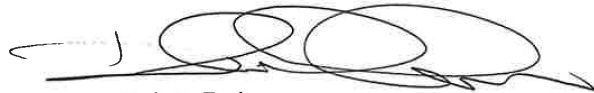
www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

Continue Improving Oversight of Third-Party Service Providers

VA ABC concurs with the audit finding. VA ABC maintains an IT Risk schedule with a focus on the more sensitive systems as a priority. Virginia ABC will review and improve the IT Risk Management Policy and document the IT Risk Management Procedures to further define the requirements for IT Risk assessments of high risk, medium risk, and low-risk systems.

VA ABC will define the System and Organization Controls (SOC) reporting requirements for high-risk vendors and for users who are storing or processing sensitive information. IT will collaborate with the Authority's procurement division to identify business owners of the services and create a review process to monitor for compliance.

Sincerely,

A handwritten signature in black ink, appearing to read 'Dale F. Farino', with a stylized flourish at the end.

Dale F. Farino



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Reported for Fiscal Year
Improve Internal Controls over Employee Separation Process	Ongoing	2022
Improve IT Risk Management and Contingency Planning	Ongoing	2023
Ensure Follow-Up Inventories are Performed	Ongoing	2024
Improve Physical and Environmental Security Policy and Processes	Ongoing	2024
Continue Improving Oversight of Third-Party Service Providers	Ongoing	2020

* A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.