VIRGINIA

ALCOHOLIC BEVERAGE CONTROL AUTHORITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2020

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

AUDIT SUMMARY

Our audit of the Virginia Alcoholic Beverage Control Authority (Virginia ABC) for the year ended June 30, 2020, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

We have audited the basic financial statements of Virginia ABC as of and for the year ended June 30, 2020, and issued our report thereon, dated December 1, 2020. Our report is included in Virginia ABC's Annual Report that it anticipates releasing in December 2020.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

Virginia ABC continues to not secure the database that supports its human resource system with certain minimum-security controls in accordance with the National Institute of Standards and Technology Standard, 800-53 (NIST Standard) and industry best practices. Virginia ABC prioritized the migration from the Virginia Information Technologies Agency (VITA) above other organizational projects and has not yet addressed the weaknesses identified in the prior year.

We communicated the continued 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 NIST Standard and industry best practices require the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Virginia ABC should prioritize efforts to ensure database configurations, settings, and controls align with its policies, the requirements in the NIST Standard and industry best practices, such as the Center for Internet Security Benchmark. Implementing these controls will help maintain the confidentiality, availability, and integrity of the sensitive and mission critical data stored or processed in the database.

Improve Security Awareness Training Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

Virginia ABC is not meeting certain requirements in the NIST Standard for security awareness training (SAT). Specifically, Virginia ABC does not have an adequate process to ensure all users complete SAT, and Virginia ABC does not require users with specific information security roles to complete role-based training. Virginia ABC has made significant progress to track security awareness training completion and has begun the process of establishing role-based training for some designated security roles. However, the following weaknesses continue to exist:

- Virginia ABC does not have an enforcement measure that requires users to take SAT. The lack of this control resulted in 15 out of 589 Central Office employees and 12 out of 2,412 Retail employees that did not take the SAT training within the past year. Virginia ABC's Information Security Officer assigns oversight of the SAT program to the Information Technology (IT) Audit Supervisor and the Human Resource (HR) Information Systems Manager. These individuals monitor whether users complete the training and send email notifications to users who have completed the training in the past year. However, Virginia ABC does not use an enforcement measure, such as disabling a user's account until training

is complete, that forces users to take the training and comply with Virginia ABC's security awareness training policy. Virginia ABC's *Security Awareness and Training Policy* requires users to take SAT within 30 days of receiving access to Virginia ABC resources and annually thereafter. Additionally, the NIST Standard requires that all computer users complete SAT initially upon employment, after significant changes in the environment, and at organizationally defined intervals thereafter *(NIST Standard section: AT-2 Security Awareness)*. Without a process to ensure that all users take SAT annually, Virginia ABC increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

- Virginia ABC does not provide role-based training to all users with designated security roles, such as system owners, data owners, system administrators, or security personnel. Virginia ABC's *Security Awareness and Training Policy* requires that personnel who manage, administer, operate, or design IT systems receive additional training commensurate with their roles and responsibilities. Additionally, the NIST Standard requires role-based training initially, when required by information system changes, and at organizationally defined intervals thereafter for personnel with assigned security roles and responsibilities (*NIST Standard section: AT-3 Role-Based Security Training*). Lack of adequate role-based training increases the risk that users will be unaware or lack pertinent skills and knowledge to perform their security related functions, increasing the risk to sensitive data.

Although the IT Audit Supervisor and HR Information Systems Manager track employees' SAT completion, approximately 25 out of 3,000 users did not complete the security awareness training in the past year. Since Virginia ABC does not document and implement a formal procedure that details the requirements and process used to track SAT completion, nor use an enforcement measure other than email notifications, Virginia ABC was unaware that these users did not complete the training. Due to the migration from VITA and other priorities, Virginia ABC also has not yet developed, documented, and implemented a process to provide role-based training to all users with designated security roles.

Virginia ABC should develop, document, and implement a formal procedure and process that includes an enforcement measure and requires all users to complete SAT training before accessing computer resources and on an annual basis thereafter. Additionally, Virginia ABC should develop a procedure and process to ensure the Information Security Officer and managers provide role-based training to users with designated security roles. Improving the SAT program will help protect Virginia ABC from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Improve Oversight of Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Virginia ABC does not employ effective processes, methods, and techniques to monitor security control compliance by external service providers (providers) on an ongoing basis. Some of Virginia ABC's providers process sensitive and mission critical information for Virginia ABC. The NIST Standard, section

SA-9(c), requires an organization to "employ organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis."

An ineffective and inconsistent ongoing process that is not documented increases the risk that Virginia ABC may inadvertently not gain appropriate assurance or have inadequate compensating controls over systems that process sensitive or mission critical information. Undocumented approvals, such as risk acceptance resulting from evaluations and presentations of risk, lack documented risk mitigation strategies that need to be available to staff for effective implementation. Documented evaluations and decisions also ensure consistency in the event of staff turnover.

Virginia ABC has a documented process to identify and manage information security risk that includes its supply chain. However, Virginia ABC does not document the process for evaluating and maintaining ongoing oversight of providers to gain reasonable assurance the providers have effective operating controls that meet established security requirements. Virginia ABC's transition from an agency of the Commonwealth of Virginia to an authority, subsequent organizational changes and responding to the COVID-19 pandemic contributed to a delay in amending and updating the process for evaluating providers.

Virginia ABC should make it a priority to update the process for evaluating providers. The update should include, but not be limited to, consistent process documentation, detailed policies and procedures, and documentation of risk acceptance evaluations. Once the update is complete, Virginia ABC should implement the policies, procedures, and processes organization wide.

Improve Internal Controls Over Terminated Employee Access Removal
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Virginia ABC is not completing off-boarding checklists or removing access for terminated employees timely. For the sample selected:

- Supervisors completed 18 of the 40 (45%) employee separation checklists between six and 80 days after the employee's termination date. It is Virginia ABC's policy for supervisors to complete checklists within five business days of termination.

- Supervisors entered terminations into Virginia ABC's human resource system between two and 111 days after the termination date. Per Virginia ABC's policy, an employee's immediate supervisor is responsible for initiating action in Virginia ABC's human resource system as soon as it is known by the supervisor, but no later than the last day at work.

- One salaried employee remained a privileged user in the Commonwealth's payroll system for 28 days after termination. Virginia ABC's policy requires a supervisor to notify the system administrator for a given system when a user no longer requires access.

Virginia ABC's human resource system generated off boarding checklists with multiple sections for completion by various departments. The five-day timeframe within the policy is specific to the section of the checklist the direct supervisor must complete. The policy does not define specific timeframes for the completion of the other sections which includes human resources, payroll, and information systems. This makes it difficult to enforce adherence to policy.

A critical function of completed checklists is to ensure the timely removal of access to Virginia ABC's systems and return of their property. Virginia ABC's untimely removal of access could result in fraudulent entries. This risk is higher for employees at Virginia ABC's headquarters with access to various human resources, financial management, or information systems; however there is also a risk associated with store employees who have access to store keys, inventory, and point of sales systems. Additionally, wage employees with access to the time and attendance system could submit fraudulent timesheets after termination.

Virginia ABC should review their current termination practices to ensure their policy is reasonable and effective internal controls are in place. Additionally, due to their unique structure, Virginia ABC should define specific procedures for retail (store) employees, enforcement employees, and headquarter employees as access levels and risks are inherently different. This will enable Human Resources to better monitor and hold supervisors accountable for timely completion of employee checklist and access removal.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 1, 2020

The Honorable Ralph S. Northam
Governor of Virginia

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

Alcoholic Beverage Control Board
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** (Virginia ABC) as of and for the year ended June 30, 2020, and the related notes to the financial statements, which collectively comprise Virginia ABC's basic financial statements, and have issued our report thereon dated December 1, 2020.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered Virginia ABC'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 Virginia ABC's internal control. Accordingly, we do not express an opinion on the effectiveness of Virginia ABC'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 entitled "Improve Database Security," "Improve Security Awareness Training Program," "Improve Oversight of Third-Party Service Providers" and "Improve Internal Controls Over Terminated Employee Access Removal," 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 Virginia ABC'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 matter that is required to be reported under Government Auditing Standards and which is described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Improve Database Security," "Improve Security Awareness Training Program" and "Improve Oversight of Third-Party Service Providers."

Virginia ABC's Response to Findings

We discussed this report with management at an exit conference held on December 7, 2020. Virginia ABC's response to the findings identified in our audit is described in the accompanying section titled "Virginia ABC Response." Virginia ABC's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

Virginia ABC has not taken adequate corrective action with respect to the previously reported findings "Improve Database Security "and "Improve Security Awareness Training Program." Accordingly, we included these findings in the section entitled "Internal Control and Compliance Findings and Recommendations." Virginia ABC has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

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 Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks

December 10, 2020

Ms. Martha Mavredes, CPA
Auditor of Public Accounts
101 N. 14th Street
Richmond, VA 23219

Dear Ms. Mavredes,

Attached are the Virginia Alcohol Beverage Control Authority (Virginia ABC) responses to the audit for fiscal year ended June 30, 2020. Virginia ABC 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 follows.

Improve Database Security

Virginia ABC concurs with this finding. Virginia ABC's primary focus has been on migrating our servers out of the Commonwealth's Enterprise Solution Center (CESC). Now that the migration is successfully complete, Virginia ABC can now prioritize ensuring that database configurations, settings, and controls align with industry standards and best practices.

Virginia ABC communicated the specific actions it will take to address the issues noted to the APA 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. Virginia ABC plans to complete these actions by March 31, 2021.

Improve Security Awareness Training Program

Virginia ABC concurs that we did not provide role-based security awareness training (SAT) to users with designated security roles as required both by the NIST Standard and our internal policy. Virginia ABC did implement some role-based training, but not specific to designated security roles. We plan to implement system owner training during FY21, and we will update our internal policy to designate the specific roles we have identified for additional training.

Although Virginia ABC did not achieve 100% completion rate for security training during the period under review, our completion rate is quite high with 97.5% for central office employees, 99.5% for retail, and 99.1% overall. Virginia ABC maintains a large part-time (PT) workforce of over 2,500 employees. These employees do not have email addresses or ready access to computer systems. With such an ever changing workforce (turnover is normally in the 40% range), it is challenging to ensure that everyone receives training within the calendar year. Virginia ABC considers 99.5% to be a successful completion rate, thereby making the use of an enforcement mechanism unnecessary. Internal controls provide reasonable assurance, not absolute assurance; it is unreasonable to expect 100% completion. Our current completion rate provides enough assurance to mitigate the potential risks described in the recommendation.

Virginia ABC has developed a process to monitor security awareness completion. While the process is not documented, its effectiveness is exemplified by the completion rate achieved. We have access to, and maintain, current lists of each employee's completion status for each module assigned. Virginia ABC's policy allows for enforcement measures, should Virginia ABC feel an enforcement measure is needed. Virginia ABC does require users to complete SAT within 30 days of onboarding, and for most full-time employees, the training is delivered when they are onboarded. Virginia ABC has developed and implemented some role-based training, and is in the process of developing and delivering training for designated security roles. Virginia ABC has a robust SAT program and we place emphasis on SAT completion, as evidenced by our over 99% completion rate for calendar year 2019.

Improve Oversight of Third-Party Service Providers

Virginia ABC agrees that we do not have documented policies, procedures, and processes specific to "ongoing" monitoring of third-party service providers. Virginia ABC should have a separate policy specific to third-party service providers that defines what constitutes a third-party service providers as well as the ongoing monitoring process. We are currently documenting that policy.

Virginia ABC's information security program is a risk-based program, not a compliance program. Virginia ABC specifically chose the NIST standard as it allows for consideration of risk, criticality, and impact. In our Information Security Risk Management policy, we require all new, replacement, and production information systems be subject to information security risk assessments. Additionally, the policy requires that third-party service provider risk assessments be identified and completed as necessary. Any service or system that is deemed to contain sensitive data, or to be mission critical, does require periodic re-assessment of risk. Virginia ABC goes beyond the NIST standard in requiring a risk

assessment for each third-party service provider; the NIST standard considers risk assessments to be an "enhanced" control, not a required control.

During the risk assessment process, Virginia ABC assesses the sensitivity of the data and criticality of the service or system to Virginia ABC's business, and the impact of failure. We determine the risk and related controls based on this assessment. Virginia ABC and the vendor then work through Virginia ABC's security requirements to identify any gaps and negotiate to address the gaps or identify compensating controls the vendor and/or Virginia ABC could employ, taking into account the cost vs. benefit of the impact. Virginia ABC evaluates any residual risk and makes a business decision whether to accept the risk or not.

Virginia ABC does document risk decisions, however, prior to FY21, that documentation took various forms. As of FY21, our project management process includes documentation of identified risks and decisions, with decision owners identified. These documents are kept as artifacts. Virginia ABC's new Third-Party Service Provider policy will include a procedure for documenting risk acceptance by management, which will be kept as an artifact with our current risk assessments.

Virginia ABC's approach to third-party service providers is a risk-based approach; this is consistent with our internal policy as well as the spirit of the relevant NIST standard. A risk-based approach inherently leaves room for management's judgement of risk. Going forward, Virginia ABC's will ensure that management's risk decisions are documented. Additionally, Virginia ABC will create and implement a policy specific to third-party service providers, which includes our process for ongoing monitoring. This policy will be completed in FY21.

Improve Internal Controls Over Terminated Employee Access Removal

Virginia ABC concurs with this finding. The Division of Human Resources, in consultation with Division of Information Technology and the Division of Finance, will review current termination practices in order to ensure reasonableness of practices and whether they are effective in establishing a strong control environment. Additionally, these divisions will review and develop access removal procedures which properly take into account risks associated with certain types of access that vary across Virginia ABC, depending on the nature of the business being conducted. Finally, Virginia ABC will continue to use email reminders to prompt managers to complete their respective portions of the checklist, while the responsible divisions undergo an analysis of existing procedures as well as development of any new procedures. Virginia ABC will complete all corrections associated with this recommendation in FY21.

Sincerely,

Travis G. Hill
Chief Executive Officer

ALCOHOLIC BEVERAGE CONTROL AUTHORITY

As of June 30, 2020

BOARD OF DIRECTORS

Maria J. K Everett
Chair

Beth Hungate-Noland
Vice Chair

Mark Rubin
Member

Gregory F. Holland
Member

William “Bill” Euille
Member

OFFICIALS

Travis Hill
Chief Executive Officer

John Daniel
Government Affairs Officer

Jerome Fowlkes
Chief Administrative Officer

Mark Dunham
Chief Retail Operations Officer

Paul Williams
Chief Information Officer

Eddie Wirt
Chief Communications and Research Officer

Thomas Kirby
Chief Enforcement Officer