



# VIRGINIA ALCOHOLIC BEVERAGE CONTROL AUTHORITY

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2019

Auditor of Public Accounts  
Martha S. Mavredes, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## AUDIT SUMMARY

Our audit of the Virginia Alcoholic Beverage Control Authority (ABC) for the year ended June 30, 2019, 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 the Virginia Alcoholic Beverage Control Authority as of and for the year ended June 30, 2019, and issued our report thereon, dated October 23, 2019. Our report is included in the ABC's Annual Report that it anticipates releasing in December 2019.

## –TABLE OF CONTENTS–

### Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-3

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

4-5

AUTHORITY RESPONSE

6-7

AGENCY OFFICIALS

8

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

### **Improve Logical Access Controls for Users with Privileged Access**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** Yes (first issued in fiscal year 2018)

ABC has not made sufficient progress since last year to update their account management processes for users with privileged access to meet the requirements in its current security standard, the Commonwealth's Information Security Standard, SEC 501 (Security Standard). In addition, ABC became an Authority in January 2018 and, as such, received autonomy from following the requirements in the Security Standard beginning October 1, 2018, and has the ability to adopt a different security standard. Therefore, ABC is in the process of transitioning to the National Institute of Standards and Technology (NIST) Standard, 800-53 (NIST Standard) as its new security standard, and is developing policies and procedures based on the NIST Standard. Thus far, ABC has a complete password policy and access control policy. The policies received management's formal approval in April 2019 and September 2019, respectively. ABC does not have accompanying procedures for the policies and they have yet to implement them into their information security program.

We addressed specific control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard and the NIST Standard requires ABC to implement specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

ABC should remediate the weaknesses discussed in the communication marked FOIAE in a timely manner, and ensure they meet all the requirements in the NIST Standard as they transition away from the Security Standard.

### **Improve Database Security**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No

ABC does not secure the database that supports its human resource system with certain minimum-security controls in accordance with the Security Standard and industry best practices.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard 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.

ABC should ensure database configurations, settings, and controls align with its policies and the requirements in the Security 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. ABC should ensure they meet all the requirements in the NIST Standard as they transition away from the Security Standard.

#### **Improve Security Awareness Training Program**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No

ABC is not meeting certain requirements in the Security Standard for security awareness training (SAT). Specifically, ABC does not have an adequate process to ensure all users complete SAT, and ABC does not require users with specific information security roles to complete role-based training.

ABC does not have an enforcement measure that requires users to take SAT. The lack of this control resulted in 120 out of 449 (approximately 27%) users who did not take the SAT training within the past year. ABC assigns oversight of the SAT program to the Information Security Officer (ISO) and the Human Resource Information Systems Manager. These individuals monitor whether users complete the training and send email notifications to users who have not completed the training in the past year. However, ABC has no other process to enforce the training requirement outside of sending the email notifications. ABC's *Security Awareness and Training Policy* requires users to take SAT within 30 days of receiving access to ABC resources and annually thereafter. Additionally, the Security Standard requires that all computer users complete SAT initially upon employment, after significant changes in the environment, and annually thereafter (*Security Standard section: AT-2 Security Awareness*). Without an adequate process to ensure that all users take SAT annually, ABC increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing and social engineering.

ABC does not provide role-based training to users with designated security roles, such as system owners, data owners, system administrators, or security personnel. 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 Security Standard requires role-based training initially, when required by information system changes, and as practical and necessary thereafter for personnel with assigned security roles and responsibilities. (*Security Standard sections: 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.

Approximately 27 percent of users did not complete the security awareness training in the past year because ABC does not have an enforcement measure, such as disabling a user's account until training is complete, that forces users to take the training and comply with ABC's security awareness training policy. In addition, although ABC requires additional role-based training, ABC has not developed,

documented, and implemented a process to provide role-based training to users with these designated security roles.

ABC should develop, document, and implement a formal process that includes an enforcement measure and require all users to complete SAT training before accessing computer resources and on an annual basis thereafter. Additionally, ABC should develop a procedure and process to ensure the ISO and Managers provide role-based training to users with designated security roles. Improving the SAT program will help protect ABC from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data. ABC should ensure they meet all the requirements in the NIST Standard as they transition away from the Security Standard.



Martha S. Mavredes, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

October 23, 2019

The Honorable Ralph S. Northam  
Governor of Virginia

The Honorable Thomas K. Norment, Jr.  
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** (the Authority) as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated October 23, 2019.

### **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 to determine the 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

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 over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled “Improve Logical Access Controls for Users with Privileged Access,” “Improve Database Security,” and “Improve Security Awareness Training Program,” 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 determination of financial statement amounts. 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 finding entitled “Improve Logical Access Controls for Users with Privileged Access.”

### **The Authority’s Response to Findings**

We discussed this report with management at an exit conference held on November 14, 2019. The Authority’s response to the findings identified in our audit is described in the accompanying section titled “Authority Response.” The Authority’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**

The Authority has not taken adequate corrective action with respect to the previously reported finding “Improve Logical Access Controls for Users with Privileged Access.” Accordingly, we included these findings in the section entitled “Internal Control and Compliance Findings and Recommendations.”

### **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/clj



Virginia Alcoholic Beverage Control Authority  
Chief Executive Officer  
Travis G. Hill



Chairman  
Jeffrey Painter  
Board of Directors  
Maria J. K. Everett  
Gregory F. Holland  
Beth Hungate-Noland  
Mark Rubin

November 1, 2019

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

Dear Ms. Mavredes,

Attached are the Virginia Alcoholic Beverage Control Authority's (Virginia ABC) responses to the audit for the fiscal year ended June 30, 2019. 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 Logical Access Controls for Users with Privileged Access**

Virginia ABC concurs with the finding. Virginia ABC will update account management of users with privileged access. Additionally, there is a concerted effort to adopt and implement the security standards now that the appropriate policies have been implemented. Virginia ABC will update our progress, on a quarterly basis, with the Virginia Department of Accounts (DOA).

**Improve Database Security**

Virginia ABC concurs with the finding and will adopt the appropriate benchmark in order to align with industry best practice and implement the controls and configurations within our capability. For any that remain, Virginia ABC will document our business need, explore mitigating, compensating controls and will pursue security exceptions as may be necessary. Virginia ABC will update our progress, on a quarterly basis, with the Virginia Department of Accounts (DOA).

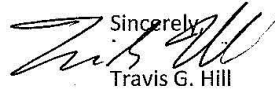
**Improve Security Awareness Training Program**

Virginia ABC concurs with the finding. Virginia ABC will require users to take annual security awareness training within a set time of assignment and will produce monthly tracking reports communicated to directors throughout the organization and quarterly reports to the Virginia ABC Board. All users who have not completed training after the set period of time will have their accounts disabled until the training is complete. Virginia ABC will also establish a program for new hires to take training as an integrated part of the current new employee orientation. Virginia ABC will also conduct role-based



www.abc.virginia.gov | 2901 Hermitage Road, Richmond Virginia 23220 | 804.213.4400

security training for all appropriate employees. Virginia ABC will update our progress, on a quarterly basis, with the Virginia Department of Accounts (DOA).

Sincerely,  
  
Travis G. Hill

Chief Executive Officer



[www.abc.virginia.gov](http://www.abc.virginia.gov) | 2901 Hermitage Road, Richmond Virginia 23220 | 804.213.4400

## **ALCOHOLIC BEVERAGE CONTROL AUTHORITY**

As of June 30, 2019

### **BOARD OF DIRECTORS**

Jeffrey Painter  
Chairman

Maria J. K Everett  
Vice Chairman

Beth Hungate-Noland  
Member

Mark Rubin  
Member

Gregory F. Holland  
Member

### **OFFICIALS**

Travis Hill  
Chief Executive Officer

John Daniel  
Government Affairs Officer

Jerome Fowlkes  
Chief Administrative Officer

Jeff Reeder  
Chief Retail Operations Officer

Paul Williams  
Chief Information Officer

Eddie Wirt  
Chief Communications and Research Officer

Thomas Kirby  
Chief Enforcement Officer