DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2014

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

AUDIT SUMMARY

We have audited the basic financial statements of the Department of Alcoholic Beverage Control as of and for the year ended June 30, 2014, and issued our report thereon, dated September 24, 2014. Our report is included in the Department's Annual Report that it anticipates releasing in December 2014.

Our audit of the Department of Alcoholic Beverage Control for the year ended June 30, 2014, 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.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Continue to Improve IT Governance

The Department of Alcoholic Beverage Control (ABC) has improved its information technology (IT) project prioritization and continues to improve its IT governance structure. While ABC has made significant efforts to implement corrective actions in response to recommendations noted during the previous audit period, various weaknesses continue to exist. We identified and communicated these 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 Commonwealth's Information Security Standard, SEC 501, requires agencies to use specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

ABC should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE that continue to align ABC's operations with industry best practices and the Commonwealth's Information Security Standard, SEC 501.

Improve Database Security

ABC does not use some required controls to protect the databases that support some critical systems in the IT environment. These databases contain sensitive information, such as personally identifiable information and operational data. We identified and communicated the weak controls to management in three separate documents marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to specific descriptions of security mechanisms.

The Commonwealth's Information Security Standard, SEC 501, requires agencies to use specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

ABC should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE and create a standard installation and configuration guide for its sensitive databases that, at a minimum, meets the requirements in the Commonwealth's Information Security Standard.

Improve Information Security Officer Designation

ABC does not position the Information Security Officer (ISO) role in an organizationally independent unit from the Chief Information Officer (CIO). The Commonwealth's Information Security Standard, SEC 501 Section 2.4.1, recommends that the ISO report directly to the agency head, where practical, and should not report to the CIO.

Having the ISO role reporting to the CIO may limit effective assessment and necessary recommendations of security controls in the organization due to possible competing priorities that sometimes face the CIO. In establishing its Information Security Officer within the organization, ABC did not fully consider the need for full independence of the Information Security Officer and the Information Security Office.

We recommend that ABC evaluate the organizational placement of the ISO to eliminate any conflicts of interest in the implementation of its information security program and controls. While it may not be feasible to have the ISO report directly to the agency head, ABC should consider placing the ISO role in a different organizational unit reporting to another executive-level position.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 24, 2014

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
Chairman, Joint Legislative Audit
And Review Commission

Alcoholic Beverage Control Board
Department of Alcoholic Beverage Control

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 **Department of Alcoholic Beverage Control** (ABC) as of and for the year ended June 30, 2014, and the related notes to the financial statements, which collectively comprise ABC's basic financial statements, and have issued our report thereon dated September 24, 2014.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered ABC'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 ABC's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of ABC'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 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 over financial reporting that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify certain deficiencies in internal control over financial reporting entitled "Continue to Improve IT Governance," "Improve Database Security," and "Improve Information Security Officer Designation," 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 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 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 matters that are 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 entitled "Continue to Improve IT Governance," "Improve Database Security," and "Improve Information Security Officer Designation."

ABC's Response to Findings

We discussed this report with management at an exit conference held on October 8, 2014. ABC's response to the findings identified in our audit is described in the accompanying section titled "Agency Response." 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

ABC has not completed corrective action with respect to the previously reported findings "Continue to Improve IT Governance" and "Improve Database Security." 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.

AUDITOR OF PUBLIC ACCOUNTS

EMS/alh

COMMONWEALTH of VIRGINIA

Department of Alcoholic Beverage Control

2901 HERMITAGE ROAD
P. O. BOX 27491
RICHMOND, VIRGINIA 23261
(804) 213-4400
FAX: (804) 213-4411
www.abc.virginia.gov

October 15, 2014

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

Dear Ms. Mavredes:

Attached are the Department of Alcoholic Beverage Control's (ABC) responses to the audit for the Fiscal Year ending June 30, 2014. As in prior years, the Department appreciates the professionalism of your staff and their diligence in assisting our Leadership Team in identifying opportunities for improvement in our internal control framework. Our responses to the findings in the Report on Internal Controls follow.

Continue to Improve IT Governance

ABC believes we have made significant progress towards an IT Governance structure as noted in the fiscal year 2013 Report. The Agency, however, continues to struggle with the ability to fund all the critical projects and still meet the long term financial obligations found in the General Assembly's Appropriations Act.

The agency's information technology (IT) governance structure is now based on industry best practices gathered through research, and policies/templates supplied by the Virginia Community College System (VCCS). ABC took the VCCS model and adapted it to meet our business needs by strengthening areas such as linkages to strategic priorities, project importance and risk management. ABC has a Technology Resource Steering Committee (TRSC) policy and accompanying materials such as process flow chart, an Excel matrix used to rank the initial round of projects, and project submission forms. Additionally, ABC has recently created a Portfolio Steering Committee that will use similar criteria to evaluate all agency projects with significant impacts.

Technology Resource Steering Committee:

The Steering Committee was chaired by the Chief Financial Officer, who has since retired; in his absence it is chaired by the Deputy Chief Operating Officer. Members currently include the Chief Information Officer, the Chief Operating Officer and representatives from two operating divisions. The Internal Audit Director serves in a non-voting capacity. Both Information Technology Project Management and Information Security have received considerable attention since last year's audit and procedures have been adopted to ensure continuous improvement.

The procedures adopted by the agency were developed to ensure that a repeatable process was in place to allocate limited technology resources (time, money and people). Information Security projects follow the same process as any other project. Members of the committee use the scoring matrix as part of the evaluation process but are also concerned with ensuring the portfolio keeps a balance between foundational and transformational projects. Considerable resources have been allocated to Information Security to ensure adequate attention is placed on areas such as risk assessments and disaster recovery planning.

While the Agency contends that standards are certainly necessary, the majority of our projects are foundational (meaning the business cannot operate without them). These include areas such as Point of Sale, the Financial System, and Licensing. In areas where return on investment (ROI) is appropriate, analysis is conducted (e.g. developing the capacity for on-line special orders.) One of the areas in significant need of improvement was increasing the agency's business analysis capability. During the last 12 months, the agency has strengthened business analysis and project management capabilities and has plans to add additional capabilities in the near future.

Project Evaluation:

The agency evaluates impacts on areas such as service to stakeholders, work process efficiency, financial costs and benefits, linkages to mandates or strategic priorities, and schedule flexibility. In the areas of risk, the agency reviews the level of certainty around scheduling, budget, complexity of the solution and the capability of the business to effectively define requirements and manage the project. As of June, some projects had been deferred because the risk threshold exceeded our comfort zone.

The technical environment for solutions is a part of the scoring matrix and is also found in scoring criteria for the procurement of customized off the shelf (COTS) products. The custom software developed at the Agency follows a standard software architecture that was developed as a common platform for each new development project.

Business Owner Involvement:

The business units are ultimately accountable for monitoring the progress on projects and the results of the implementation. The transition from an IT centric to a business centric approach is on track to be successful (as evidenced by the reports presented by the business owners at progress meetings). Business owners must describe how projects link to agency strategies and goals as part of the submission process. Every two months, the project owners present to the TRSC on schedule, scope, costs and risks.

Additionally, the Agency recognizes the need for system owners to implement security controls in the project development process. Better communication and security presence has been injected into the project process where possible and in a just-in-time manner with job aids being produced to re-educate IT and the business community.

Finally, forthcoming efforts by the security team are eminent (including re-education of business owner roles and responsibilities), that will result in captured and monitored metrics to ensure that compliance requirements are known and measured.

Use of Agency Resources:

The Agency has also invested resources into a Board requested project to evaluate the current staffing needs and approve new positions where applicable including an additional business systems analyst and a pending position for an IT Compliance Analyst to support the Governance, and risk Compliance initiatives.

Improve Database Security

ABC currently has several applications that are running on an outdated database platform version. ABC has reviewed the applications that utilize the database and assessed that the applications, in their present state, will not support a database platform upgrade without a significant and unacceptable impact to the business. Given that the database platform is no longer supported, and changes to the database may introduce unpredictable results, editing settings and/or configurations may result in unacceptable downtime or lack of recovery for the application and the database.

ABC Executive Management made a decision to accept the risks of the current applications until a new ERP solution can be implemented. ABC purchased Breach Insurance in March 2014, which further mitigates the impact of a security incident. ABC is in the process of filing an exception with the Virginia IT Infrastructure Partnership (VITA) and should have documented approval of the exception to the Security Standard once the filing has been approved.

For one of the applications residing on the database, ABC has enlisted a third party vendor (Oracle Consulting) to perform a gap analysis and produce a mitigation strategy for the new system. For another application, ABC has defined requirements and is in the process of vendor selection, with negotiations currently underway with one vendor. Due to the cost and complexity of this system, it is expected to take approximately 2 years before the final solution is implemented.

With regards to certain settings and permissions on the database and application accounts, ABC has made changes where changes were possible to be made without extensive testing or risk to the business. In other instances, while the agency concurs the settings are not compliant, a thorough analysis and testing period will need to occur to determine any risk of editing these settings. The Agency commits to this research and will change any settings where the risk is minimal. Settings changes that would negatively impact the business will be discussed with the System Owner. Risk will either be mitigated or accepted. And finally, ABC has a valid business need for certain roles not to be in compliance with SEC 501. ABC has accepted the risk and will implement the strongest controls the business need will allow. These exceptions are included with the VITA Exception filing currently in process.

Improve Information Security Officer Designation

ABC will evaluate the organizational placement of the Information Security Officer (ISO) in order to remove the perception of any conflicts of interest in the implementation of our information security program and controls. ABC has a newly appointed Chief Operating Officer (COO) as of Monday, October 6, 2014. Once the new COO has had a chance to become acclimated, ABC will begin an evaluation of the best placement for the ISO within the organization, whether as a direct report to the COO or placement elsewhere within the organization. Although ABC will require the input of the new COO for final determination, we expect the process to take 90 days or less. Once a decision has been reached ABC will notify the APA.

Sincerely,

Jeffrey L. Painter
Chairman

DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL BOARD MEMBERS

As of June 30, 2014

Jeffrey Painter
Chairman

Judy Napier
Commissioner