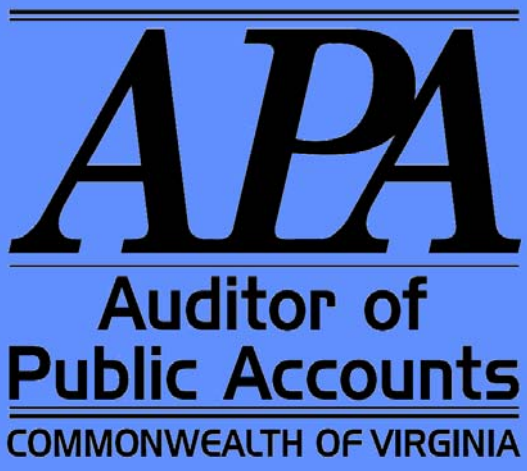
DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2010



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, 2010 and issued our report thereon, dated September 28, 2010. Our report is included in the Agency's Annual Report that it anticipates releasing on or around December 1, 2010.

Our audit of the Department of Alcoholic Beverage Control for the year ended June 30, 2010, found:

- the financial statements are presented fairly, in all material respects;
- certain matters that we consider to be significant deficiencies in internal control; 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 FINDINGS AND RECOMMENDATIONS

Improve Systems Access Processes and Monitoring

In our prior audit, we found the Department of Alcoholic Beverage Control (Department) does not perform system access security reviews in compliance with its information security program. The Department has made limited progress addressing this recommendation; however, based on our review of access, we believe the Department should make system access security reviews a priority.

The Department does not maintain adequate documentation for many of its systems on what roles allow users to access what data or perform what functions within their systems. Many of the Department's system are several years old and the capabilities of the system to identify roles have become dated, due to organizational changes and the implementation of other systems.

Not having this documented could lead to users having access to systems that they do not need or users receiving excessive access. Additionally, multiple users share administrative accounts that grant access to the entire system. Sharing accounts removes accountability for employees' actions, as it is virtually impossible to determine what actions a specific employee has taken while they are using a shared administrative account.

The Department risks allowing inappropriate access to sensitive data without adequate reviews and access role configurations documented. The approvals should be performed by individuals with the appropriate technical knowledge, such as the Information Security Officer (ISO). In addition, the Department risks undetected, unauthorized access or changes to systems and data due to the shared administrator accounts and the undocumented roles to the various systems within the Department.

The ISO should develop and implement a method to review users' access across all systems. The ISO should also work with system owners to fully document their access roles within the systems. The Department should also eliminate the sharing of administrator accounts and all users needing administrator access should have their own account. Lastly, the Department may need to dedicate resources to allow the ISO to ensure compliance with its information security program.

Use Automated Workflow Process

The Department has the opportunity to improve its operational efficiency by using automated workflow process for the entering and approving of transactions in their general ledger system. Also, the Department could streamline its process for obtaining and reconciling information between systems, which results from not having automated system interfaces.

The manual approval of entries into the general ledger system does not provide the level of internal control as required in an automated process. Review and approval of hardcopy supporting documentation provides no assurance over the accuracy of the system recorded information. This form of approval increases the risk of inaccurate and inappropriate transactions and the risk that employees will circumvent controls.

The Department should either implement automated workflow with adequate segregation of duties in the Performance System or restructure and assign user roles to prevent users from entering and approving their own transactions. Either of these options will provide stronger controls, a more efficient process, and a reduction in paperwork by automating the entire process.

The reconciliations are time consuming, but without an automated transfer of data between systems, they are essential. The ability to change information before transfer can result in misstatements, or accidental modification of data. We recommend that ABC analyze all system feeds to determine where there are opportunities to increase efficiencies automating the transfer of data, thus removing the need for reconciliations.

Improve Information Technology Policies and Procedures

The Department's information security program continues to lack consistency across all sensitive systems. As noted last year, the Department has documented policies and procedures for security over its critical data in accordance with the Commonwealth's Information Security Standard; however, the Department has not made it clear that some of these policies and procedures only apply to certain systems.

Communicating a consistent information security program is essential to ensuring that users of the systems understand their responsibility in protecting sensitive data, no matter the system. When security requirements and expectations differ greatly among the systems, the Department risks inconsistent application and enforcement of those requirements. There are some instances, such as with systems that process credit card information, where more stringent security requirements are necessary. Additionally, any systems that are not segregated from those that process credit card data must also comply with more stringent security requirements.

We recommend that the Department streamline its security policies and procedures so that they clearly delineate the policies and procedures that apply to all systems from those security policies and procedures that only apply to specific systems. We also recommend that the Department ensure these policies apply to all systems that both directly process credit card information as well as other systems that access credit card information indirectly.

Improve Database Security Monitoring

The data owner and database administration staff do not consistently review database audit logs. Logging database activity and reviewing the logs consistently allows data owners to ensure the integrity of data and gives assurance that there are no unauthorized changes. The Department's logging policies and procedures do not specify the types of database activities to track, the frequency of the reviews, and who has responsibility for reviewing logs, or responding to suspicious activity.

The Department should improve its policies and procedures for logging and monitoring to include requirements for logging of high-risk activities, frequent and regular reviews of logs by appropriate individuals, and procedures for documenting and responding to suspicious activity. Detailed and specific policies and procedures are essential to ensuring the Department can communicate and enforce expectations and responsibilities of its staff for the security of critical and sensitive data. When developing a strategy for regular log reviews, the Department should consider risk to Department operations and sensitivity of data in determining how often to perform log reviews.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

September 28, 2010

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable Charles J. Colgan
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 the basic financial statements of the **Department of Alcoholic Beverage Control** as of and for the year ended June 30, 2010, and have issued our report thereon dated September 28, 2010. We conducted our audit in accordance with 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.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the Department's internal control over financial reporting as a basis for designing our auditing procedures 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 Department's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Department'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.

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 deficiencies, significant deficiencies, or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies entitled "Improve Systems Access Process and Monitoring" and "Use Automated Workflow Process," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies in internal control over financial reporting. 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.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Department's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contract 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. Instances of noncompliance and other matters, entitled "Use Automated Workflow Process," "Improve Information Technology Policies and Procedures," and "Improve Database Security Monitoring", are described in the section titled "Internal Control and Compliance Findings and Recommendations."

The Department's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit the Department's response and, accordingly, we express no opinion on it.

Status of Prior Findings

The Department has not taken adequate corrective action with respect to the previously reported findings "Improve Systems Access Processes and Monitoring," "Improve Information Technology Policies and Procedures," and "Improve Database Security Monitoring". Accordingly, we included these findings in the section entitled "Internal Control and Compliance Findings and Recommendations." The Department has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Report Distribution and Exit Conference

The "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters" is intended solely for the information and use of the Governor and General Assembly of Virginia, the Alcoholic Beverage Control Board, and management, and is not intended to be and should not be used by anyone, other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We discussed this report with management at an exit conference held on October 18, 2010.

AUDITOR OF PUBLIC ACCOUNTS

CGC/clj

COMMONWEALTH of VIRGINIA

Department of Alcoholic Beverage Control

2901 HERMITAGE ROAD
P O BOX 27491
RICHMOND, VIRGINIA 23261
PHONE (804) 213-4400
FAX (804) 213-4411
TDD LOCAL (804) 213-4687

October 26, 2010

Mr. Walter J. Kucharski
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, VA 23219

Dear Mr. Kucharski:

The Virginia Department of Alcoholic Beverage Control appreciates the opportunity to comment on the Auditor of Public Accounts most recent audit report for ABC. This letter provides ABC's response to the internal control findings and recommendations noted during the audit of our 2010 financial statements. ABC strives to maintain an effective system of internal controls over financial reporting and operations and is pleased that the report contains no significant findings and focuses on best practice suggestions using national benchmarks. The report did contain 4 recommendations relating to information security: 1) Improve Systems Access Processes and Monitoring; 2) Use Automated Workflow Process; 3) Improve Information Technology Policies and Procedures; 4) Improve Database Security Monitoring.

ABC strongly believes that it has consistently maintained an effective information systems security program and welcomes the opportunity to continually strengthen our program in light of the ever changing information security environment. Listed below are the Department's responses to the recommendations.

Improve Systems Access Processes and Monitoring

ABC, like many agencies in the Commonwealth, has a series of legacy systems, many of which have been in existence for years. User roles documented at the time of implementation or creation may have evolved over the years as the employee roles and duties have changed, and ABC's written documentation of these changes has not kept pace with actual practice. ABC agrees that it needs to review user access and user roles, and clearly document those user roles, for each sensitive system owned.

ABC has begun the process of user role review and documentation for its general ledger and POS systems and will continue with each sensitive system until all roles have been clearly documented. ABC is also developing a review program to ensure there is a process in place for periodic user access review for all ABC systems. ABC will revise our current policies to include this provision and the ISO will ensure that the program includes an analysis of access roles and user access.

ABC will review administrative accounts on all systems and ensure appropriate individual accountability is defined. Where administrative rights are shared, ABC will create separate accounts for each administrative user.

Use Automated Workflow Process

While ABC concurs that automating the workflow in our general ledger system will provide efficiencies, ABC currently has an effective internal control system in place to ensure transactions are accurate. ABC's general ledger system, Performance, is a 12 year old legacy system, and until the system can be replaced, ABC must work within its confines and limitations. ABC is currently automating the workflow process to the extent possible within the system. The automation will eliminate the need for manual approval of entries, with a mechanism for ensuring appropriate segregation of duties. ABC, while exploring additional functionality for its general ledger system, is also reviewing and redefining user roles.

ABC has already analyzed all system feeds because we recognize the possibility for data manipulation or accidental modification; we identified this issue previously and have been working to address it. As a compensating control, ABC does perform reconciliations of the data that is transferred between the systems to ensure data integrity. ABC is currently in the Quality Assurance testing phase of a solution to prevent modification of the data during the file transfer process that should be completed and in place by November, 2010.

The new process of transferring secure files should ensure the integrity of the data from one system to the next as it will no longer be able to be manually manipulated, however, ABC will continue to reconcile the data between systems. While ABC agrees that in some respects, an automated transfer of data through a system to system interface may introduce some efficiencies, it would not alleviate the need for reconciliations. Any exchange of data, whether manual or automated, should be reconciled to ensure data integrity between systems. Both manual and automated processes are subject to error without proper monitoring. ABC believes in a strong system of internal control and believes that regular reconciliations between systems are an inherent part of the internal control system.

Improve Information Technology Policies and Procedures

ABC has two Information Security policies in effect: a policy to ensure Payment Card Industry (PCI) compliance that is specifically for those systems that process credit card information, and a policy for our systems that do not need to meet the extremely stringent requirements of PCI compliance. ABC believes these policies, and their applicability, are consistent and clearly communicated within ABC. ABC has, however, drafted a new Information Security policy that is awaiting Board approval. The updated policies (PCI and Information Security) clearly separate the credit card environment from the remaining systems.

Improve Database Security Monitoring

ABC currently follows best practices for database logging and monitoring, and will incorporate our current practices into our formal written security policy. ABC will ensure the policy specifies the types of database activities to track, the frequency of the reviews, and who has responsibility for reviewing logs or responding to suspicious activity.

ABC would like to restate again its commitment to an effective information security program. We will continue to make this a priority and allocate the necessary resources to ensure the continued protection of the Commonwealth's data. As always, we appreciate the diligence and professionalism of your staff along with the opportunity to respond.

Sincerely,

J. Neal Insley

Copy: The Honorable Marla G. Decker, Secretary of Public Safety

DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL BOARD MEMBERS
As of June 30, 2010

J. Neal Insley
Chairman

Sandra C. Canada

Wayne J. Ozmore, Jr.