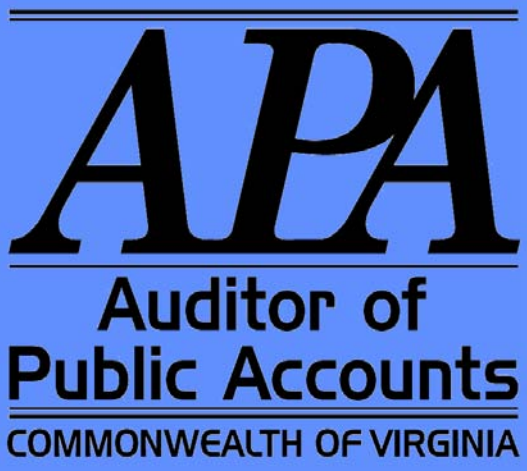
DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2009



AUDIT SUMMARY

We have audited the basic financial statements of the Department of Alcoholic Beverage Control (Department) as of and for the year then ended June 30, 2009, and issued our report thereon, dated September 28, 2009. Our report is included in the Department of Alcoholic Beverage Control's Annual Report that it anticipates releasing on or around December 1, 2009.

Our audit of the Department of Alcoholic Beverage Control for the year ended June 30, 2009, 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
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

– T A B L E O F C O N T E N T S –

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Compliance with Information Security Program

The Information Security Officer does not perform system security reviews in compliance with the Department's information security program. The Department has charged the Information Security Officer with developing an information technology security review, compliance and risk management program in conjunction with Internal Audit for random information security assessments. However, the Information Security Officer has not followed the Department's policy to develop an information system security evaluation process with Internal Audit in order to minimize the risk of improper user access to sensitive data.

The Information Security Officer should work with Internal Audit to establish efficient audit plans to evaluate whether the information security program is effective. Part of the review with Internal Audit should include reviewing access role configurations in sensitive systems to ensure roles provide adequate segregation of duties. The Information Security Officer should conduct reviews of user access at least annually for all sections of the Department having access to financial or sensitive systems. The Department should dedicate the resources necessary to allow the Information Security Officer to ensure compliance with the information security program.

In addition, the Information Security Officer should periodically review the audit logs for inappropriate access to all sensitive systems. The Information Security Officer should review user account requests for sensitive systems subsequent to the review and approval by data owners.

Improve Database Security

The Department does not provide adequate oversight to mitigate risks of unauthorized access to critical data. The data owner and database administration staff do not regularly review user access to databases or audit logs of database activity. In addition, the data owner and database administration staff do not follow the Department's policies and procedures for password controls for administrative accounts on one of its critical databases.

The Department should perform regular reviews of user access to databases to include user roles and permissions to modify data, tables, and application code. The Department should develop and implement a strategy for logging database activity, reviewing logs regularly, and responding to suspicious activity. The Department should implement password controls on databases that comply with both Department policies and the Commonwealth's Information Security Standard. The Department should document exceptions to its password policy in the cases of system and application accounts where the password controls may affect system functionality.

The Department has already taken the first steps in addressing these issues by purchasing a new server and upgrading its application. Unlike the old application, the new application is capable of handling the requirements of current information security standards and industry best practices. We encourage the Department to continue to address these issues in their application and database environments.

Improve Information Security Program

The Department's information security program lacks consistency across all sensitive systems. 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 with sensitive data.

The Department should 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 with sensitive data. The Department should ensure that these policies and procedures apply to systems that process credit card information as well as other systems that are not segregated from systems with credit card information.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

September 28, 2009

The Honorable Timothy M. Kaine
Governor of Virginia

The Honorable M. Kirkland Cox
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, 2009, and have issued our report thereon dated September 28, 2009. 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.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or

detected by the entity's internal control over financial reporting. We consider the deficiencies, which are described in the section titled "Internal Control Findings and Recommendations," to be significant deficiencies in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in the internal control over financial reporting that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that the significant deficiencies described above are not material weaknesses.

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, 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 no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

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 finding "Oracle Database Security." Accordingly, we included this finding in the section entitled "Internal Control Findings and Recommendations."

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 19, 2009.

AUDITOR OF PUBLIC ACCOUNTS

RNW: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
TDD LOCAL (804) 213-4687

October 21, 2009

Mr. Walter J. Kucharski
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Mr. Kucharski:

This letter provides the Department of Alcoholic Beverage Control's response to the management points identified during the audit of our 2009 financial statements. Thank you for the thorough review of our financial statements and information systems. The audit resulted in three findings relating to Information Security: 1) Improve Compliance with Information Security Program, 2) Improve Database Security and 3) Improve Information Security Program. Listed below are the Department's responses to the findings.

Improve Compliance with the Information Security Program

The Information Security Officer (ISO) will develop a review program in conjunction with Internal Audit to determine the effectiveness of our information security program. ABC will revise our current policies to include this provision and the ISO will ensure that the program includes analysis of access role configurations, user access, and analysis of audit logs for inappropriate access to sensitive systems.

Improve Database Security

ABC currently uses OSSEC, an Open Source Host-Based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response, for PCI compliant systems review. ABC will expand its use of OSSEC to all sensitive systems.

Several of the potential issues identified specifically address database logging, roles, permission reviews, and other security monitoring. While indicated as a repeat finding, the 2008 finding, "Oracle Database Security", pertained to one system and ABC completed the necessary corrective action in September 2009. ABC's efforts to rectify that issue were delayed by 11 months due to issues with the VITA/NG partnership. ABC

Remediated the issue within one week of the Partnership's fulfillment of our requirements. ABC agrees with the 2009 updated recommendations as indicated in your report, and have already implemented several improvements during the course of the audit. ABC will revise and develop policies and procedures to ensure that all recommendations included in the APA finding: "Improve Database Security" are implemented.

Improve Information Security Program

ABC concurs with the APA's finding: "Improve Information Security Program". ABC is in the process of segregating credit card systems from other systems through the deployment of administrative PC's in its retail outlets, and through the use of Windows firewalls in its central operations.

As always, we appreciate the diligence and professionalism of your staff along with the opportunity to provide comments for your report.

Sincerely,

Susan R. Swecker, Chair
VA Department of Alcoholic Beverage Control

SRS

AGENCY OFFICIALS

BOARD MEMBERS
As of June 30, 2009

Esther H. Vassar
Chairman

Susan R. Swecker

Franklin P. Hall