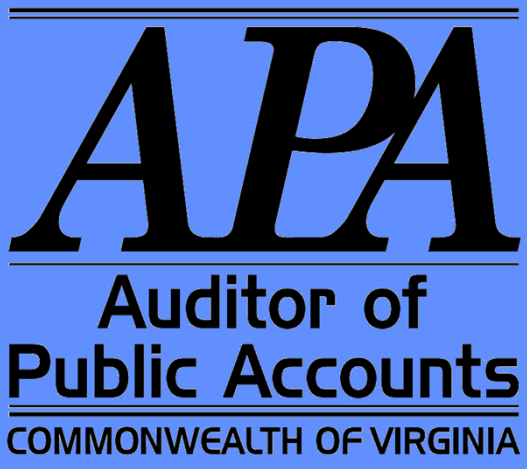
DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2011



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, 2011 and issued our report thereon, dated September 28, 2011. Our report is included in the Department's Annual Report that it anticipates releasing on or around December 1, 2011.

Our audit of the Department of Alcoholic Beverage Control for the year ended June 30, 2011, found:

- the financial statements are presented fairly, in all material respects;
- certain matters involving 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.

- T A B L E O F C O N T E N T S -

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve User Account Controls

The Department of Alcoholic Beverage Control (ABC) neither deletes disabled user accounts nor reviews disabled user account activity. While certain access restrictions would prevent non-system users from improperly using these accounts, a knowledgeable insider could use the lack of account monitoring and not deleting the accounts to take advantage of this lack of control to improperly circumvent the system without detection. Most breaches of information security and loss of data and assets comes from insiders taking advantage of the system.

ABC's data retention policy requires the removal of disabled user accounts from Information Technology (IT) systems after three years. However, ABC is not enforcing its data retention policy nor is ABC monitoring disabled user account access to ensure that no one has improperly used the accounts. Both the monitoring and the eventual removal are essential internal controls to protect information and assets. Therefore, we recommend that ABC dedicate the necessary resources to delete disabled user accounts and monitor disabled user accounts for unusual activity. ABC also needs to re-evaluate its current three year user account retention policy and develop a policy where the timeframe is commensurate with the risk identified in its IT risk assessment and business impact analysis.

Improve Remote Store Server Security

ABC does not comply with the industry best practice and Commonwealth's security standard minimum configuration requirements on their Point of Sale servers. We have communicated the details of these weaknesses to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of the security system.

We recommend that ABC utilizes a compliance validation tool to determine an appropriate baseline for the POS server configuration security settings. Additionally, we recommend that ABC configure all of their remote store servers in accordance with Center for Internet Security best practices and the Commonwealth's Information Security Standard, SEC501-06.

Improve Compliance with Information Security Program

ABC has not performed system access reviews for SEIS, CORE, MyABC, or MOVE, which are four of the department's 13 major systems, during the fiscal year. Without adequate reviews and approval of users and their access role configurations by System Administrators or by individuals with technical knowledge and authority within the agency, such as the Information Security Officer (ISO), ABC risks allowing inappropriate access to sensitive data. Inappropriate access puts ABC at risk for undetected, unauthorized changes to systems and data due, and can lead to fraud and abuse.

In our prior audit, we noted that ABC was not performing system access security reviews in compliance with its information security program and acknowledge that ABC has made limited progress on this issue. The ISO should develop and implement a method to systemically review user's access across all major systems annually and all other systems at least every two years. Further the ISO should dedicate the necessary resources to achieve this compliance. Since bringing this matter to the attention of the Security Officer, he has begun addressing these systems.

Commonwealth of Virginia

Auditor of Public Accounts

Walter J. Kucharski
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 28, 2011

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, 2011, and have issued our report thereon dated September 28, 2011. 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

Management of the Department is responsible for establishing and maintaining effective 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 Remote Store

Server Security," "Improve Compliance with Information Security Program," and "Improve User Account Controls," 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, 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 "Improve Compliance with Information Security Program." Accordingly, we included this finding 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 14, 2011.

AUDITOR OF PUBLIC ACCOUNTS

WJK: clj

COMMONWEALTH of VIRGINIA

Department of Alcoholic Beverage Control

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

October 19, 2011

Mr. Walter Kucharski
Auditor of Public Accounts
James Monroe Building
101 North 14th Street
Richmond, Virginia 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 2011 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 or financial-related findings. The report did contain three recommendations relating to information security: 1) Improve User Account Controls; 2) Improve Remote Store Server Security; and 3) Improve Compliance with Information Security Program. ABC does not concur with Finding 1, concurs with Finding 2, and partially concurs with Finding 3.

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 User Account Controls

ABC does not concur with this finding. Retaining disabled accounts is required by the Commonwealth in both the Information Security Standard (SEC 501-06) and the Records Retention and Disposal Schedule of the Library of Virginia. ABC intentionally retains disabled accounts to maintain the integrity of its historical transactions because the accounts are tied to audit records, and removing the accounts would lead to orphaned records.

The Information Security Standard, ITRM SEC 501-06 (Rev 4/11), published by the Virginia Information Technologies Agency (VITA), Section 5.2.2: Logical Access Control Account Management Requirements, specifically states:

> *"Each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:*
>
> *12. Disable unneeded accounts.*
>
> *13. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy."*

ABC is in the process of developing record retention schedules for each system. Not all records are retained for three years; some records are retained for longer periods of time. The three year policy discussed with the APA was referencing the Library of Virginia Records Retention and Disposition General Schedule No. 113 which addresses account access. Other Library of Virginia Schedules reference different retention periods – the period is dependent upon the specific data being retained. For data with a longer retention periods, deleting accounts after three years would violate policy. Additionally, the timeframe is "x" number of years after no longer required, not from creation. For example "Contract and Agreement Records" (GS-101 Series 100312) says "Retain 5 years after termination". A contract may last 10 years, in which case the record (and, in theory, related accounts) would be 15 years old before destroyed.

Reviewing disabled user account activity is not required by the standards and would require significant system architecture/design changes, would require significant investment, and would be of negligible value. In order to be used, the account must be re-enabled, in which case reviewing "disabled" accounts would show no activity. ABC has internal controls built into its various sensitive systems that prevent or mitigate the risk of a current employee enabling a disabled account and being able to improperly use it. For example, in order to reactivate and use an account in MyABC, ABC's Human Resource System, a Personnel Action Notice would need to be generated and approved by the HR manager or director.

ABC is required by the Commonwealth's IT Standards, and the Library of Virginia, to disable accounts and retain those accounts for the same time period required by its data retention policy. While we welcome the Auditor of Public Accounts' opinion, we respectfully disagree. ABC is in compliance with the required Standards and has invested considerable resources in internal controls to prevent unauthorized use of accounts. We believe that dedicating resources to review disabled accounts is not an efficient use of ABC's resources and would provide little benefit for the costs involved.

Improve Remote Store Server Security

ABC concurs with this finding.

ABC plans to address several outstanding known issues as part of a current Center for Internet Security (CIS) remediation project. All issues that will be addressed are expected to be completed by March 1, 2012. For the remaining issues, ABC has reviewed the server configuration and has legitimate business need for

most of the requirements that have not been met. For these, ABC will identify risks for the business owners to accept, document mitigating controls, and file SEC501 exceptions. The anticipated date for risk documentation and exception filing is March 30, 2012.

Improve Compliance with Information Security Program

ABC agrees that the agency is not completely in compliance with its Information Security program, however, the agency has made significant progress over the fiscal year since the 2010 audit. A consultant was hired to address issues with the InfoSec program, and a complete rewrite of the Policies, Standards, and Guidelines was created. The ABC Board approved the new program, and implemented an Information Security Steering Committee to provide governance oversight to the program and ensure value delivery. Additionally, the Board was provided the necessary training for security functions and system definition; sensitivity was reviewed and updated; and a Business Impact Analysis was completed. Significant advances were made in the vulnerability management program, including a Commonwealth-leading application vulnerability remediation program.

In compliance with the Information Security Roadmap project underway, which has been approved by the ABC Board and provided to the APA, additional System Owner documentation has been completed to assist in the InfoSec program compliance. A completely revamped training program is currently being developed for System Owner, Data Owner, and System Administrator roles. Additional risk management and individual system security projects and documentation will be completed in Q2 and Q3 FY2012.

As for the specific systems noted in the finding, ABC did complete access reviews for MOVE. These access reviews are completed quarterly and signed by System Owner. The documentation was provided to the APA on 8/12/2011. SEIS did not have access reviews at the time of the audit, but access reviews have since been completed and processes implemented to ensure continual compliance in the future. MyABC and CORE have not yet had access reviews completed; these are large systems and a single point of contact could not effectively evaluate access. A procedure is being implemented that will ensure the correct individuals review access and that these reviews are documented.

ABC would like to restate again its commitment to an effective information security program. We have and 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, Chairman

APA'S COMMENTS ON MANAGEMENT'S RESPONSE

Retaining user accounts in a disabled state after an employee's termination introduces the risk for fraud. An account may be re-enabled, used to process a transaction, and disabled again. Without an internal control to detect whether disabled accounts have been used to process transactions, the department may not timely detect fraudulent transactions.

Our recommendation relates to those systems not yet migrated into "Account Central," ABC's new system to centrally manage and monitor user accounts. While Account Central has the proper controls to manage user accounts, ABC does not have a project plan that outlines when all their sensitive systems are supposed to be migrated.

After considering ABC's response, our opinion remains the same. We recommend that ABC implement controls to detect the increased risk of fraudulent transactions resulting from maintaining accounts in a disabled state.

DEPARTMENT OF ALCOHOLIC BEVERAGE CONTROL BOARD MEMBERS
As of June 30, 2011

J. Neal Insley
Chairman

Sandra C. Canada