Thomas P. DiNapoli
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

February 10, 2010

Mr. Dennis Rosen
Chairman
Division of Alcoholic Beverage Control
State Liquor Authority
Alfred E. Smith Building
80 South Swan St. - Suite 900
Albany, NY 12210

Re: Report 2009-F-45

Dear Mr. Rosen:

According to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution; and Article II, Section 8 of the State Finance Law, we followed up on the actions taken by officials of the Division of Alcoholic Beverage Control (Division), to implement the recommendations contained in our audit report, Network Security Controls (Report 2008-S-111).

Background, Scope and Objective

The New York State Legislature enacted the Alcoholic Beverage Control Law in 1934 to regulate the State's alcoholic beverage industry. The Alcoholic Beverage Control Law created the State Liquor Authority and the Division of Alcoholic Beverage Control (Division). The State Liquor Authority is a three member board, consisting of a chairman and two commissioners, which oversees the work done by Division staff. The Division has two main functions: issuing licenses and ensuring compliance with the Alcoholic Beverage Control Law.

The Division has a computer network (Network) to help carry out its duties. The Division's Data Processing Unit maintains the Network. This includes supporting all servers, configuring hardware, setting up desktop computers, supporting software, providing Network connectivity for all business units, and managing Network devices.

The Division must comply with the New York State Office of Cyber Security and Critical Infrastructure Coordination's Cyber Security Policy. The Security Policy defines minimum information security requirements that all State agencies must meet and requires State agencies to establish a framework to manage its own information security.

Since the original audit, the Division has hired a new Chief Executive Officer and Director of Internal Audit.

Our initial audit report, issued on January 29, 2009, examined the security controls over selected aspects of the Division's computer network. We identified certain areas in which the controls needed to be improved. The objective of our follow-up was to assess the extent of implementation as of January 28, 2010 of the ten recommendations included in our confidential report. Due to the sensitivity of the information and the potential risk associated with the release of such information, the details of the recommendations and their implementation status are not included in this report. However, we discussed the detailed results of our follow-up work with Division officials.

Summary Conclusions

We found Division officials have made progress toward implementing many technical recommendations. However, they have not implemented the more critical recommendations for building a strong security foundation at the Division. For example, neither a risk assessment nor a data classification has been completed. Both are needed to determine what the most critical data is, where it is stored and how it should be protected. In addition, Division officials have not developed benchmarks to ensure information security controls are working. Division officials agreed with our conclusions and indicated that they will take additional actions to fully implement our recommendations.

Major contributors to this report were Nadine Morrell, Claudia Christodoulou, Jennifer Van Tassel, and Corey Harrell.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We also thank the management and staff of the Division for the courtesies and cooperation extended to our auditors during this process**.**

Yours truly,

Brian Reilly
Audit Manager

cc: Ms. Alison Pingelski, Director of Internal Audit
Mr. Thomas Lukacs, Division of the Budget