THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

December 14, 2016

Ms. Margaret Miller
Chief Information Officer
Office of Information Technology Services
Empire State Plaza
Box 2062
Albany, NY 12220

Re: Security and Effectiveness of
Department of Motor Vehicles'
Licensing and Registration Systems
2016-F-15

Dear Ms. Miller:

Pursuant 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 have followed up on the actions taken by officials of the Office of Information Technology Services to implement the recommendations contained in our audit report, *Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems* (2013-S-58).

Background, Scope, and Objectives

The Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State Information Technology Transformation to consolidate and merge State agencies and streamline information technology services. The consolidation of agency information technology employees was organized by cluster and arranged by the type of service the agency provides. The Department of Motor Vehicles (Department) was initially part of the former General Government Cluster, which has been renamed the Citizens Services Cluster (CSC) and is comprised of 12 agencies. A draft Customer Operating Agreement effective January 1, 2016 through December 31, 2016, outlines the services to be provided by ITS to agencies that receive their primary technology support through CSC. The agreement documents the responsibilities of both the customer and ITS.

The Department uses 419 software products and 219 system applications administered by ITS to fulfill its mission. During 2016, more than 9,700 users interacted with the license and registration processing, which generated $793.8 million in revenue during fiscal year 2015-16. In that same time period, more than 7.6 million credit card transactions were processed by the Department.

Our initial audit report, which was issued on September 19, 2014 covering the period of November 14, 2013 through June 27, 2014, determined whether the Department's licensing and registrations systems were secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap that disables normal processing. We found that ITS and the Department were not in full compliance with Payment Card Industry (PCI) Data Security Standards that govern the systems that process credit card transactions. We also found ITS did not comply with certain State cybersecurity policies and did not establish adequate processes for managing user access of Department systems. The objective of our follow-up was to assess the extent of implementation, as of August 15, 2016, of the five recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

ITS made progress in implementing the recommendations identified in our prior audit report. However, we found that in several instances, although new processes were instituted, security controls over certain Department licensing and registration systems still need material improvement. Of the five prior recommendations, two have been implemented and three have been partially implemented.

Follow-Up Observations

Recommendation 1

Prioritize Cluster initiatives to include completion of appropriate tasks in order to reach compliance with PCI Data Security Standards.

Status – Implemented

Agency Action – ITS provided a PCI Data Security Standards Report on Compliance dated December 31, 2015 and signed by Department executive management and an independent PCI Qualified Security Assessor. The report certified that Department systems now meet PCI Data Security Standards.

Recommendation 2

Create Enterprise-wide and resultant aligning Cluster policies that address logging and user access control.

Status – Implemented

Agency Action – The Enterprise Information Security Office issued NYS-S14-005: Security Logging standard in February 2014, which replaced two logging policies that pre-dated ITS. This standard defines requirements for security log generation, management, storage, disposal, access, and use for several different types of security events. These events include successful and unsuccessful authentication, privileged operations, access to log

files, and unsuccessful resource access. In addition, on August 15, 2014, the Enterprise Information Security Office issued NYS-S14-013: Account Management/Access Control standard, which addresses user access controls by establishing rules and processes for creating, maintaining, and controlling the access of a digital identity to New York State applications and resources.

Recommendation 3

Create, maintain, and monitor a log of patches applied to Department software to ensure timely completion.

Status – Partially Implemented

Agency Action – Our review found that ITS has an adequate patching process for workstations. However, due to the recent migration of Department servers to the State's new data center, ITS is still working to ensure all servers are patched in a timely manner or the appropriate controls are implemented for those servers that it is unable to patch timely. ITS officials also advised the audit team that they are implementing additional security controls and increasing audit exception logging, where possible.

Recommendation 4

Continue to move forward toward the implementation of a complete and viable change management and user access management process that will provide adequate controls.

Status – Partially Implemented

Agency Action – ITS has a documented Enterprise-Wide Change Management policy, and the CSC has documented change management procedures that support this policy. ITS uses ServiceNow software to administer its change management process. However, according to ITS officials, ServiceNow does not allow ITS or Department officials to ensure all implemented changes have gone through the approved change management process and are recorded. To provide adequate controls, ITS is developing a configuration management database which will flag exceptions and create a report when changes are applied without using ServiceNow. Without established controls to ensure that all changes adhere to the established process, ITS cannot demonstrate that the process is working as intended.

ITS also has an Enterprise-wide user access policy and associated processes for both general user access and database user access. However, ITS was unable to provide documentation to support the controls surrounding the provisioning and de-provisioning of access, despite several requests from the audit team. ITS officials stated they have "two in-flight projects that will consolidate and rationalize the storage of user data, and the processes to provision and de-provision users."

Recommendation 5

Develop and implement a succession plan, including Assembler and COBOL program language

training, to ensure continuity of Department operations and service.

Status – Partially Implemented

Agency Action – During our prior audit, ITS officials told auditors a large modernization plan had been developed that "would address many of the older technologies through service-oriented architecture and a master data migration." At that time, officials did not provide us with a copy of this plan and, due to ITS's delay in responding, auditors were unable to review it. ITS did provide auditors with the modernization plan during our current review. While the plan contains guiding principles for modernization and refers to the need to deploy more modern web-based technologies, it does not specifically note any plans to address the shortage of staff with Assembler and COBOL expertise. Further, officials indicated there are no imminent plans for replacing COBOL programs; rather, aspects of how users access these applications will be modernized.

In addition to the modernization plan, officials provided auditors infrastructure remediation plans, a timeline of DMV modernization through December 2017, and employee training logs for the three most recent employees hired with job duties that include programming in Assembler and COBOL. The training logs provided were dated more than three years ago, and one log was last updated in 2009, which pre-dated ITS and was five years prior to the issuance of our audit. In addition, the CSC recently finalized a standard which provides specifications for writing new COBOL code or modifying existing COBOL code. While this standard supports ITS's initiative to train, document, and provide ongoing support to existing employees, it does not address a succession plan to ensure ITS is able to maintain adequate employee resources to address infrastructure written in Assembler and COBOL programming languages. ITS officials expressed confidence that the "modernization efforts underway will reduce the dependency on Assembler and COBOL and eventually result in systems being modified to ITS preferred technology."

Major contributors to this report were Nadine Morrell, Mark Ren, Jared Hoffman, Holly Thornton, and Molly Kramm.

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 Office for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

John F. Buyce, CPA, CIA, CFE, CGFM
Audit Director

cc: Rajni Chawla, ITS Internal Audit Director
Division of the Budget