New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems

Office of Information Technology Services

Report 2013-S-58 September 2014

Executive Summary

Purpose

To determine whether the Department of Motor Vehicles' (Department) licensing and registration systems are secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap that disables normal processing. This audit covers the period November 14, 2013 through June 27, 2014.

Background

The New York State Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies and is headed by a Chief Information Officer. ITS' Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. ITS organized approximately 40 executive branch agencies into nine clusters based on the type of service provided. The Department is one of eight agencies that comprise the General Government Cluster (Cluster). The Department uses 147 IT systems and 265 software products, most of which are used to process driver licenses and vehicle registrations. In addition, the Department processes more than 6 million credit card transactions annually, totaling almost $700 million, for license and vehicle registration processing. During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal and credit card data stored in the Department's systems, maintaining compliance with applicable security standards, and ensuring continuity of effective and efficient operations.

Key Findings

- ITS and the Department are not in compliance with the Payment Card Industry (PCI) Data Security Standards that govern the systems that process credit card transactions. Since January 2012, neither agency has completed and submitted a required self-assessment questionnaire or third-party compliance report, which are necessary to ensure that all risks have been properly identified and mitigated. Non-compliance also exposes the State to other risks ranging from extensive fines or penalties to business disruption due to cancelled accounts and the inability to accept credit card payments.
- ITS does not have an established monitoring and oversight process for user access management of Department systems and is not operating in compliance with State cybersecurity policies.

Key Recommendations

- Prioritize Cluster initiatives to include completion of appropriate tasks in order to reach compliance with PCI Data Security Standards.
- Create Enterprise-wide and resultant aligning Cluster policies that address logging and user access control.
- Create, maintain, and monitor a log of patches applied to Department software to ensure timely completion.
- Continue to move forward toward the implementation of a complete and viable change

management and user access management process that will provide adequate controls.

Other Related Audits/Reports of Interest

Office for Technology: Procurement and Contracting Practices (2010-S-71)
Office of Information Technology Services: Procurement and Contracting Practices (2013-F-24)

State of New York
Office of the State Comptroller

Division of State Government Accountability

September 19, 2014

Mr. Brian Digman
NYS Chief Information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Dear Mr. Digman:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by so doing, providing accountability for tax dollars spent to support government-funded services and operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit of the Office of Information Technology Services entitled *Security and Effectiveness of the Department of Motor Vehicles' Licensing and Registration Systems*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this draft report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies, combining talent and assets from various agencies to foster innovation, build skills, and promote development in order to meet customer needs. To achieve this, ITS organized the IT employees from approximately 40 executive branch agencies, accounting for more than 4,000 employees, into nine clusters based on type of services provided: Environment and Energy, Financial, Administrative and General Services, General Government, Health, Human Services, Disability and Aging, Public Safety, and Transportation and Economic Development. ITS' objectives include consolidating cluster infrastructure operations for each agency cluster and improving cluster effectiveness and integration.

ITS is headed by a Chief Information Officer. There is also an Enterprise Operations Group headed by the Chief Operating Officer, which is responsible for delivering centrally managed IT services to the agencies. The Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. EISO has assumed the functions, powers, and duties of the former Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), including governance, compliance and risk management, incident response and digital forensics, security monitoring and intelligence, vulnerability and threat management, secure systems engineering and architecture, security training and awareness, and cluster security services. In addition, the EISO is responsible for setting statewide security policies and developing standards for use by all State agencies. The EISO is revising the State's cybersecurity policies currently in effect, issued by the former CSCIC, in order to establish baseline standards and policies with which all clusters' policies must align. ITS standards and policies will follow the framework of the National Institute of Standards and Technology.

The Department of Motor Vehicles (Department) is one of eight agencies that comprise the General Government Cluster. The Department issues secure identity documents, delivers essential motor vehicle and driver-related services, and administers motor vehicle laws enacted to promote safety and protect consumers. To accomplish its objectives, the Department uses 147 IT systems and 265 software products, most of which are used to process driver licenses and vehicle registrations. In addition, the Department processes more than 6 million credit card transactions annually, totaling almost $700 million in revenue for license and vehicle registration processing. More than 4,000 users interact with the Department's computer systems, which also provide Internet-based customer service access.

During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal and credit card data stored in Department systems, maintain compliance with applicable security standards, and ensure continuity of effective and efficient operations.

The General Government Cluster management (Cluster) issued a strategic plan outlining and

prioritizing Cluster-wide initiatives. In addition, the Cluster maintains a service-level agreement, which details the IT services and support provided to the eight agencies on behalf of ITS. According to the agreement, the Cluster is responsible for providing software and systems support to the Department as well as service management of core processes, including change management and incident management; disaster recovery planning; administration of Payment Card Industry (PCI) standards; hardware support services, including mainframe administration and patch management needs; software support services, including the maintenance of an approved software catalog and handling of system outages; and managed network support services, including user access provisioning. Department officials remain responsible for the administration of its Business Continuity planning.

Audit Findings and Recommendations

To determine whether the Department's licensing and registration systems are secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap, we evaluated a range of system controls, including compliance with security standards, access management, change management, and system uptime. We found that ITS systems, which process Department transactions, are not in compliance with PCI Data Security Standards, and identified several other critical areas - specifically patch management, change management, and user access management - in need of improvement. We also found that ITS has not always established adequate control over its processes and procedures during the transition.

ITS is in its second year of transformation and many of its Enterprise policies, and resultant Cluster-level policies, are still under development. We noted that before the transformation began, ITS did not conduct an underlying risk assessment to identify potential policy conflicts or other procedural issues among agencies, which could thereby assist with a smooth transition. As a result, employees have had to rely on some of their former agency policies and procedures, increasing the risk that critical functions and procedures are not consistently handled among the Cluster agencies. It is imperative that ITS ensure that appropriate processes and controls continue to be followed as State entities transition from agency-specific policies to Enterprise-developed policies in order to minimize the risk of weakened operations and disruption in quality of service.

We also examined system uptime to determine the stability of the systems used to process Department transactions and found that ITS systems satisfactorily address this issue. We also evaluated disaster recovery and Business Continuity processes and found these areas to be working as expected. Finally, we noted that ITS needs to have a better succession plan in place to address impending constraints it faces with the older programming languages used.

Payment Card Industry Data Security Standards

Industries that accept credit cards as a method of payment must comply with Data Security Standards established by the PCI Security Standards Council to protect against electronic security breaches and theft of payment card data. The PCI Standards are enforced by the five global payment brands - American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Depending on their annual transaction volume and the payment brands' respective requirements, merchants are required to submit certain forms of compliance verification to each payment brand annually. The Department is required to submit to each payment brand either a third-party annual report on compliance or an annual self-assessment questionnaire.

We found the ITS systems that process Department payment transactions have been out of compliance with the current PCI Data Security Standards since January 2012, and within this time frame neither the Department, prior to the transformation, nor ITS since has submitted the required third-party annual report or self-assessment questionnaire to the payment brands. Absence of these third-party reports and self-assessments reduces the level of assurance that

all appropriate risks have been identified and mitigated. In addition, non-compliance increases the Department's exposure and risk of extensive fines from the various payment brands as well as business disruption and other operational consequences, which could range from cancelled accounts and the inability to accept credit card payments to security weaknesses and potential lawsuits.

Department officials began working toward compliance in 2011, prior to the transformation. Progress toward compliance continued under ITS after the transformation; however, the projected completion date has continually changed due to resource constraints and other project initiatives. In response to our preliminary findings, Cluster officials contend that the Department will now reach compliance with PCI Data Security Standards by the latest version's effective date deadline of January 1, 2015.

User Access Management

ITS does not always have sufficient controls in place to properly manage user access to Department systems and is not operating in compliance with policy.

Mainframe System

We found ITS failed to establish processes governing the use and oversight of its mainframe security software, jeopardizing the integrity, confidentiality, and security of the Department's information assets. ITS uses the security software for control over user access to the mainframe where all confidential licensing and registration data, including customers' personal information, is stored. It tracks access activity based on user IDs that it has assigned, which currently number more than 3,000. In response to our preliminary findings, officials noted that they follow general user access guidelines. However, during our discussions with ITS employees responsible for this software, they noted that there are no written policies governing the use of the software that controls access to the mainframe.

According to the cybersecurity policy, access to State-entity IT equipment, systems, and networks must be provided through the use of individually assigned unique identifiers. We found that 181 of 3,007 user IDs are not assigned to a particular individual as required by the policy. We also determined that some of the created user IDs have never been used and others have not been used in more than 12 years, compromising accountability and the ability to trace activities to the responsible party.

In response to our preliminary findings, officials noted that those IDs not assigned to a particular individual are generally service accounts used by the system and application processes. Other exceptions include restricted-use accounts for access to lower-security limited-use software products, diagnostic tools, batch processes, etc. However, due to the lengthy delay in receiving this response (one month after the audit's closing conference), auditors were unable to verify this assertion.

Other Systems

For some systems, ITS has no assurance that user access control data is accurate and reliable, that systems are being accessed only by authorized individuals, and that the information being communicated to and from Cluster management and Department staff is accurate.

As of March 7, 2014, the software the Cluster relies on to manage user access to Department systems became unsupported. Prior to this date, ITS allowed the version of software used by the Cluster to become outdated, and as a result they are now unable to upgrade to the current version since it is no longer supported by the vendor. In response to our findings, Cluster officials noted that, despite being outdated and unsupported, the software is still functional and, in their opinion, poses a low risk. Cluster officials informed us that ITS has procured a new software program which they will eventually use to address user access management needs. However, our review found this program currently cannot handle user access management, and Cluster officials were unable to provide documentation to support when this capability will be available.

To determine whether user access data is accurate, reliable, appropriate, and up to date, we selected a sample of 50 active and 50 non-active employees and examined their access rights. We found that the user access software data showed 18 percent (9 of 50) of the retired, transferred, or terminated employees in our sample still had open access to Department systems. However, in response to our findings, ITS officials noted only one still had access to a domain account which allows users access to a system based upon their permissions, and this has been disabled as a result of our audit.

In addition, our testing showed that eight employees continued to have open access to a certain type of network security access device beyond the date when their access was supposed to have expired: more than two years for two employees and over one year for the remaining six. Further, we found ITS can't be assured that all information communicated to and from Cluster management and staff is accurate. For example, when the audit team questioned officials regarding these access issues, the Cluster CIO first stated that this particular security device was no longer used and as a result, even if employees still had open access to it, they would not be able to use it. However, in a response to our preliminary report, Cluster officials revised their position and stated that, with the exception of one of the users who turned their device in and has not had access in two years, the security device was still actively used. These conflicting statements are indicative of the level of confusion that we encountered as we tried to identify precisely which policies and procedures are in effect and who is responsible for their implementation and monitoring.

Software Patching and Change Management

The Department uses 265 different software products in over 21 categories of software programs. These software products run on several different operating systems. According to ITS policy, all system software must be maintained at a vendor-supported level to ensure software accuracy and integrity. Further, the maintenance of State entity-developed software must be logged to ensure changes are authorized, tested, and accepted by management. Given the vast number

of software products the Department uses for its operations, as the procedure for logging and documenting changes transitions from a Department-specific process to one that aligns with the draft ITS Enterprise processes, it is critical that the Cluster have proper controls over software and system maintenance. However, we found the Cluster has failed to properly log all patches and changes made to Department software and systems. As a result, Department software may be vulnerable to security incidents and corruption, which could negatively affect the confidentiality, integrity, and availability of Department data and impair software integrity.

Despite our repeated requests, Cluster officials did not provide any documentation to support the logging of patches to any of the Department's operating systems. When we questioned the ITS official in charge of patching the Microsoft operating system, we were told there was no official log maintained. In response to our preliminary findings documenting this statement, Cluster officials countered that they use the System Center Configuration Manager to document patches applied to Microsoft products. However, this does not address patches to other operating systems and software products in use.

Without a log documenting applied patches, Cluster officials cannot be certain that all the appropriate patches have been applied in a timely manner and that software integrity is intact. Rather, the Cluster is forced to rely on vulnerability scans and vendor notifications instead of the logs as mandated by the ITS and DMV policies. We selected a sample of 43 of 265 software programs used to determine if the version in use was up to date. We found that 60 percent (26 of 43) of the software is at a version below what is currently offered by the vendor and 44 percent (19 of 43) is no longer supported. In response to our findings, ITS officials noted that a transition is underway to an enterprise tool that will establish a more consistent and managed inventory.

The procedure for logging and documenting changes to Department systems is also transitioning from a Department-specific process to one that aligns with the draft ITS Enterprise processes. The Enterprise is in the process of creating a universal policy for change management for all the clusters, and the Cluster is the first pilot cluster to attempt to implement change management.

As with our review of access management controls, in response to our inquiries about the Cluster's change management process, we were directed to a series of different agency contacts and were repeatedly given conflicting information. Toward the end of our audit, we were referred to the Cluster's 'Acting' Change Manager, who took on this duty in March 2014, several months after our audit began. The Change Manager provided us with logs that the Cluster now uses to document system changes. We found that, although the Department started using the logs as early as January 2014, it wasn't until late March 2014 that it began actually recording essential change management information concerning priority, classification, approval, and success.

In response to our preliminary findings, Cluster officials referred us to additional documentation, including copies of blank checklists that had been components of the Department's change management process prior to the transformation. Once again, the conflicting information and apparent confusion at several levels is an indication that ITS officials need to improve coordination efforts to ensure that appropriate actions are taken during this time of transition, and to implement a strong, transparent oversight process documenting implemented change requests.

Ease and Efficiency

All licensing and registration data the Department processes is stored on their mainframe, which was programmed primarily using the older programming languages Assembler and COBOL. According to ITS officials, these languages are currently still supported, and they also have started using newer and more relevant programming languages. The pool of individuals who are proficient in Assembler and COBOL is shrinking, particularly as employees who are well versed in the aging mainframe programming languages enter retirement. To ensure the Department's mainframe operates without interruption due to this diminishing resource, it is essential that ITS have a succession plan in place to address impending constraints.

For example, ITS was unable to provide the audit team with a plan to address the inevitable shortage of staff with Assembler and COBOL expertise. By failing to plan appropriately, ITS could risk disruption to, or impairment of, Department systems that rely on these older programming languages. However, one ITS official told auditors there was no real need for preparation and training, expressing confidence that ITS has enough staff who know the older languages and that anyone could simply open a book and learn how to use a programming language anyway.

In contrast, after our fieldwork was completed and about one month after our closing conference, in response to our preliminary findings, officials noted that "most recently there has been the development of a large modernization plan that will further address many of the older technologies through service-oriented architecture and master data migration." ITS officials did not provide us with a copy of this plan and, due to ITS' delay in responding, auditors were unable to review it.

Disaster Recovery and Business Continuity

Our tests showed the Department's Business Continuity planning processes are comprehensive and complete. We also found ITS' Disaster Recovery process properly includes testing of the mainframe and supporting servers that process license and registration data. The audit team found these tests are being conducted sufficiently.

However, we also noted that the location and condition of the current data center which houses the Department's mainframe and supporting servers has some physical control weaknesses, including water pipes that run vertically and above the mainframe and server equipment, the use of an individual universal power supply instead of a facility-wide unit, and the lack of an emergency shutdown. In addition, although the Department contends the system is inspected semi-annually, staff couldn't provide documentation to demonstrate such frequency. Rather, ITS provided one inspection dated December 2012 and another dated March 2014. The most recent inspection was conducted two weeks after our walkthrough.

It should be noted that the Department plans to relocate to a new data center, and that this move should address these physical weaknesses. However, ITS officials were not able to provide information on precisely when the move will take place.

Recommendations

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

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

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

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.

5. Develop and implement a succession plan, including Assembler and COBOL program language training, to ensure continuity of Department operations and service.

Audit Scope and Methodology

We audited the security, effectiveness, and long-term sustainability of core Department IT systems at ITS for the period November 14, 2013 through June 27, 2014. The objective of our audit was to determine whether the Department's licensing and registration systems are secure, operating effectively, and available to continue processing in the event of a disaster or mishap that disables normal processing.

To accomplish our objective, we interviewed selected ITS and Department officials and staff to obtain an understanding of ITS Enterprise, Cluster, and Department policies and procedures and to obtain an understanding of internal controls relevant to security and effectiveness of the computer systems. To complete our audit work, we reviewed supporting documentation for user access, business continuity, disaster recovery, PCI security, change management, and uptime in order to determine compliance with established policies. We selected a sample of active and non-active employees from the 2,686 active users and 120 non-active users to examine their access rights. We also made visits to data center locations.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to

certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed 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.

Reporting Requirements

We provided a draft copy of this report to ITS officials for their review and formal comment. We considered their comments in preparing this report and have included them in their entirety at the end of it. In their response, ITS officials indicated that certain actions have been and will be taken to address the report's recommendations. Our rejoinders to certain ITS comments are included in the report's State Comptroller's Comments.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chief Information Officer shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and if the recommendations were not implemented, the reasons why.

Contributors to This Report

John Buyce, CPA, CIA, CFE, CGFM, Audit Director
Brian Reilly, CFE, CGFM, Audit Manager
Nadine Morrell, CISM, CIA, CGAP, Audit Supervisor
Holly Thornton, Examiner-in-Charge
Patrick Lance, Staff Examiner
Dylan Spring, Staff Examiner
Mark Womeldorph, Staff Examiner
Marzie McCoy, Senior Editor

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

ANDREW M. CUOMO
Governor

Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

August 26, 2014

Brian O. Reilly
Audit Manager
Office of the State Comptroller
Division of State Government Accountability
110 State St
Albany, NY 12236

RE: Draft Audit
Security and Effectiveness of DMV Licensing and Registration Systems
Report 2013-S-58

Dear Mr. O'Reilly:

Please allow this letter to respond to the Draft Audit Report 2013-S-58 issued by the Office of the State Comptroller (OSC) concerning the security and effectiveness of the Department of Motor Vehicle's licensing and registration systems (the Draft Report). We believe that these responses provide an accurate reflection of how IT Transformation is progressing and its relation to DMV's systems specifically.

Clarification of ITS Organization (Background):

The transformation is large, complex and in progress. Accordingly, ITS seeks to make the following clarifications to the descriptions of its organization in the Draft Report.

As indicated in the Draft Report, the Office of Information Technology Services (ITS) was established as part of a New York State IT transformation to streamline and modernize the delivery of information technology (IT) by the State. This was effected on November 22, 2012 when the IT professionals from approximately 40 executive branch agencies were transferred to ITS.

ITS organized its IT professionals into roughly two types of service delivery organizations: centrally managed IT services, such as infrastructure services, directed by a Chief Operating Officer (COO); and cluster-based IT services, which are directed by a Cluster Chief Information Officer (CIO). The COO and the Cluster CIOs all ultimately report to the NYS CIO. Each cluster is made up of IT professionals who support a group of agencies. Agencies are grouped into clusters based on similarities between their core missions. The clusters are: Environment and Energy, Financial, Administrative and General Services, General Government, Health, Human Services, Disability and Aging (formerly known as "Behavioral Health"), Public Safety, and Transportation and Economic Development.

* Comment 1

* See State Comptroller's Comments on Page 20.

ITS is headed by the NYS Chief Information Officer. The Draft Report states that ITS is also headed by "an Enterprise Operations Group" and that the Enterprise Operations Group oversees the clusters. This is not correct. As described above, the Enterprise Operations Group is directed by ITS's COO, who reports up to NYS CIO, and it is responsible for delivering centrally managed IT services, such as infrastructure services, to customer agencies. The COO's Enterprise Operations Group does not oversee the clusters. Rather, it works with cluster IT staff to ensure that the customer agencies receive the full breadth of IT services they need. The clusters are each overseen by a Cluster CIO who is ultimately responsible to the NYS CIO.

* Comment 1

The Draft Report mentions DMV's continued responsibility for the administration of its Business Continuity planning. DMV also continues to be responsible for setting priorities of, and dedicating funding for, DMV-related IT projects.

Audit Findings and Recommendations:

ITS takes the security and effectiveness of all of the systems it operates, including DMV's, very seriously and welcomes the insight, input and recommendations offered by the auditors. While this Draft Report focuses on DMV alone, it is worth noting that on November 22, 2012, ITS instantly became responsible for the operation, security, deployment, patching and management of the legacy products, systems and applications that grew up over the decades in the 40+ different agencies and their varied environments. The point of IT Transformation is for ITS to harmonize these disparate management processes and policies that flourished in these 40+ agencies and establish a consistent set of best practices to be leveraged across all of them. The Draft Report reflects this context. For example, it notes that "[t]he procedure for logging and documenting changes to the [DMV] systems is also transitioning from a [DMV]-specific process to one that aligns with the draft ITS Enterprise processes." (Draft Report at page 10). As part of its core mission, ITS is in the process of creating and establishing enterprise-level, best practices that can be leveraged across all agencies, hence the "draft" ITS Enterprise process referred to in the Draft Report. In the meantime, ITS is continuing to use the legacy DMV-specific process that had existed within DMV prior to transformation. DMV, and all of ITS's customer agencies, are partnering closely in this effort and ITS considers extensive and objective reviews, such as this audit, essential to our success.

- **Payment Card Industry (PCI) Data Security Standards:**

As set forth in our March 20, 2014 responses to OSC's preliminary audit findings report (the "March 20, 2014 Responses"), DMV continues to make PCI Data Security Standards compliance a high priority and both DMV and ITS implemented and continue to implement many types of measures all aimed at mitigating any possible risk of vulnerability exploitation.

As set forth in our March 20, 2014 Responses, PCI Data Security Standards Version 2 was released prior to IT Transformation in October 2010 with a compliance deadline of January 2012. In response to the release of Version 2 standards, DMV contracted with Grant Thornton, a Qualified Security Assessor, to assess DMV's compliance and provide a gap analysis to aid in creating a plan to attain compliance with Version 2. Grant Thornton's assessment stated that:

> DMV has done an excellent job of implementing the majority of the technical and administrative controls required by the PCI DSS where the system or network was scoped correctly….Appropriate logging and monitoring systems are in place to alert personnel to security issues.

> Data is encrypted properly and delivered to Global Payments (DMV's then-payment processor) in a secure manner. And regular reviews of authorized personnel who have access to the system and data is performed. Similarly implemented effective controls exist for the Real @dvantage point of sale system as well as paper based transaction processing."

Grant Thorton advised DMV to reduce the number of systems and locations where payment card data is processed and transmitted in order to lessen the time and cost of achieving and maintaining PCI Data Security Standards Version 2 compliance.

Since the assessment, DMV IT staff have been transferred to ITS and PCI Data Security Standards Version 3 has been issued. Version 3 compliance is required by January 1, 2015. Still, ITS and DMV were on track to be compliant with PCI Data Security Standards with Global Payments as the payment processor. However, the Global Payments centralized contract was replaced with a new vendor, Key Merchant Services (KMS). The contract transition from Global Payments to KMS adversely impacted ITS and DMV's compliance schedule as contract finalization stretched. More delays occurred when it became apparent that the new vendor could not provide all of the services DMV needed and had originally obtained from Global Payments.

Notwithstanding the contracting delays, ITS and DMV continue to work closely with Grant Thornton on their recommendations and, as stated in ITS's March 20, 2014 Responses, ITS and DMV expect to be compliant with PCI Data Security Standards Versions 2 and 3, as required by the payment brands. DMV, which continues to be responsible for prioritizing and funding its agency IT-related projects, has always made, and continues to make, PCI compliance a highest priority.

Finally, OSC is correct in that neither DMV (prior to IT Transformation) nor ITS (since IT Transformation) have been able to submit reports and assessments to the payment brands. That, however, in and of itself, does not increase the risk that a vulnerability exists thereby putting cardholder data in "jeopardy." It is important to reiterate that while these reports have not been submitted, DMV and ITS have implemented a litany of measures -- a controlled system environment, policies, procedures, standards, compensating controls, web application firewalls, logging applications, encryption and code reviews – all of which reduce the likelihood of an exploitation of a vulnerability. To this end, OSC did not find that DMV's system had a vulnerability or an exploit thereof.

- **User Access Management**

Some of the findings made about User Access Management in the Draft Report are not particularly detailed making them difficult to respond to. For example, OSC found that ITS "failed" to establish processes for governing the use and oversight of mainframe security software. It is not clear what this finding is based on since OSC only referred to inconsistencies among staff on the existence of written procedures. Otherwise, in our March 20, 2014 responses to OSC's preliminary audit findings report, ITS explained in detail how it manages and tracks user access to systems. Specifically, for ITS-DMV systems, such systems currently follow a standard User Account/Access (UAM) process. Similar to many system administration tasks managed by ITS Service Management, RACF (Resource Access Control Facility) user-ID's are currently administered by the ITS Systems Programming group through the standard UAM process defined that triggers workorder requests by the Service Desk. The UAM process, and the associated procedure for RACF account administration for RACF User Account Management was previously shared with

* Comment 2

OSC in our preliminary response to this portion of the audit. The UAM process involves immediate disable of the DMV domain/network logon when a user is de-provisioned, as well as the removal of the RACF account. In addition to the targeted and limited functions available to mainframe users (for example SAS users can only access SAS reports), if exceptions occur, there are a number of controls that reduce the risk of mainframe account access (e.g. specialized and configured 3270 software is required, the user interface is not intuitive and requires mainframe knowledge, a domain/network account is pre-requisite). Periodic review and deletion of unneeded accounts is performed to address exceptions or service accounts that remain when systems are retired. RACF user ID's that are not assigned to a particular individual are generally service accounts, used by the system and application processes. Other exceptions include restricted use accounts for access to lower-security limited use software products, diagnostic tools, batch processes, etc. RACF account administration is tightly controlled with provisioning performed by a limited number of specialized ITS system programmers. A RACF health check was recently performed, and a list of recommendations was developed and prioritized. The list and the remediation plan update was shared with OSC in a ITS-DMV preliminary response on this topic.

- **Software Patching and Change Management**

As set forth above, as part of its core mission ITS is establishing enterprise-level, best practices that can be leveraged across all customer agencies. In the meantime, ITS is continuing to use the legacy DMV-specific processes and tools that had existed within DMV prior to transformation. For example, and as stated in the ITS preliminary responses, ITS is using the System Center Configuration Manager to document patches for Windows systems. For other operating systems and software products in use there is a mix of automated tools that perform software patching and some that are applied manually. Due to the volume it is difficult for ITS to holistically address the patching across all software due to interdependencies and underlying risks of incompatibilities. The current focus is on the higher risk and security related vulnerabilities and we are working to increase the use of automated tools as we work to align our supported software with ITS standards.

* Comment 3

- **Ease and Efficiency**

In the Draft Report OSC references the use of older programming languages and acknowledges that the pool of resources with knowledge of these programs is shrinking. Modernizing our systems is a priority for both ITS and its customer agencies, including DMV. To be sure, ITS has had conversations directly with the auditors' principals at OSC regarding efforts to modernize certain IT systems. That said, DMV systems that rely on these older programming languages are functioning well and OSC made no findings that these systems are insecure or ineffective based on the code language they employ.

* Comment 4

- **Disaster Recovery and Business Continuity**

In the Draft Report OSC found that the location and condition of the data center that currently houses DMV's systems has some physical control weaknesses. In the Draft Report, OSC also acknowledged that DMV has plans to relocate to a new data center. ITS has begun the process of moving DMV to the new data center. For example, archive storage files are in the process of being migrated to the data center, and all new systems are being constructed there. This process is ongoing, and while ITS is making every effort to ensure this process is completed in an efficient

and expedited manner, our goal of ensuring that the process is also done properly and in accordance with best practice necessitates flexibility in the implementation timeframe.

* Comment 5

As to OSC's five recommendations, we have the following response:

1. **Recommendation 1**: DMV continues to make PCI Data Security Standards compliance a priority and DMV and ITS will continue to work together to meet the PCI target compliance date.

2. **Recommendation 2**: ITS continues to generate and update its policies and standards around security, many of which are posted publicly on the ITS website. For example, on or near August 15, 2014, ITS EISO published a policy on Enterprise Account Management/Access Control.

3. **Recommendation 3**: ITS will continue to work with its customer agencies, including DMV, on establishing an enterprise-grade, best practices to log patches.

4. **Recommendation 4**: ITS will continue to move forward with the implementation of a complete and viable change management and user access management process that will continue to provide adequate controls.

5. **Recommendation 5**: ITS will continue to work with its customer agencies to prioritize system modernization.

Thank you for the opportunity to respond to this draft audit.

Sincerely,

Theresa Papa

Theresa Papa
Director of Administration

State Comptroller's Comments

1. Based on ITS' response, we amended our report to better reflect the Enterprise Operations Group duties and responsibilities. Additionally, we revised the agency participation number and a Cluster name.
2. During the course of our audit, the audit team requested procedures for mainframe user access and were informed that none existed. It was not until the preliminary response dated June 27, 2014 that ITS officials stated that general user access procedures were also used to govern mainframe user access. Further confusing the issue, officials, in their response to the draft report, reference a March 20, 2014 preliminary response, a date prior to the preliminary issuance. Although officials contend that a periodic review and deletion of unneeded accounts is performed, they failed to address those user IDs identified in the report that either have never been used or have not been used in more than 12 years. In addition, the RACF health check provided in response to our preliminary findings and referenced as recently performed was dated April 27, 2012, more than two years prior, and it only contained a plan without documentation to support that it was ever actually operationalized.
3. ITS officials did not provide any evidence or state that they use any mix of automated tools to perform software patching for operating systems other than Windows. During the audit, officials informed us that they used vulnerability scans to verify that a patch has been applied.
4. As noted in our report, after our fieldwork was completed and about one month after our closing conference, in response to our preliminary findings, officials noted that "most recently there has been the development of a large modernization plan that will further address many of the older technologies through service oriented architecture and master data migration." However, ITS officials did not provide us with a copy of this plan. Further, no other conversations regarding DMV modernization efforts were held with ITS officials. Rather, discussions revolved around a subsequent ongoing audit of ITS' Unemployment Insurance Systems at the Department of Labor. To date, ITS officials have still not provided the requested information on that modernization project.
5. Auditors requested a timeline of transfers to the new data center and did not receive the schedule until long after the fieldwork was complete on this audit. In fact, we received the referenced schedule in relation to a subsequent audit of ITS systems at the Division of Criminal Justice Services. The schedule indicates that the earliest date of completion will be June 2015.