Department of Motor Vehicles
2015 **SLAA REPORT**

March 8, 2016

Brian Kelly, Secretary
California Transportation Agency
915 Capitol Mall, Suite 350-B
Sacramento, CA 95814

Dear Mr. Kelly,

In accordance with the State Leadership Accountability Act (SLAA), the Department of Motor Vehicles submits this report on the review of our systems of internal control and monitoring processes for the biennial period ended December 31, 2015.

Should you have any questions please contact Bernard Soriano, Deputy Director, at (916) 657-7626, bernard.soriano@dmv.ca.gov.

BACKGROUND

The Department of Motor Vehicles (DMV) is a department within the California State Transportation Agency. With a workforce of more than 9,500 employees, DMV provides driver license and identification card services to 28 million customers and registration services for 33 million vehicles. DMV provides services to more customers than any other state department.

The mission of the DMV is to serve the public by providing quality licensing and motor vehicle-related services. The DMV principal core functions are:

Driver License and Identification Card Program: Test and issue licenses to qualified drivers, provide identification services to the public and verify the identity of all licensed drivers and identification card holders.

Vehicle Title and Registration Program: Issue titles and register all automobiles, motorcycles, trailers and vessels, as well as commercial vehicles for both interstate and intrastate commerce. Issue disabled person placards and personalized license plates.

Licensing of the Motor Vehicle Industry: Provide customer protection through the licensing and regulation of occupations and business related to the manufacture, transport, sale and disposal of vehicles, including: vehicle manufacturers, dealers, registration services, salespersons, transporters, and dismantlers.

Driver Safety Program: Promote traffic safety by monitoring the driving performance of licensed drivers. We evaluate high-risk drivers for driving competency and take corrective actions against the driving privilege of drivers who demonstrate safety risks.

The New Motor Vehicle Board is a program within the Department of Motor Vehicles with oversight provided by the California State Transportation Agency. The mission of the New Motor Vehicle Board is to enhance relations between dealers and manufacturers throughout the state by resolving disputes in the new motor vehicle industry in an efficient, fair and cost-effective manner.

RISK ASSESSMENT PROCESS

DMV performed the risk assessment utilizing training workshops, meetings and interviews with DMV staff and management at all levels. The DMV Enterprise Risk Management (ERM) Division facilitated a series of training workshops over several months which included DMV staff of each of the DMV divisions. A

series of three workshops of two hours each were conducted which focused on key areas of risk analysis and evaluation.

The workshops generated risks at the divisional and enterprise level. The risk assessment did not focus on one specific area. ERM looked throughout the department for input from management and staff to identify and evaluate areas of risk. Management and staff within each division were given an opportunity to reflect, discuss risks, and explain mitigating controls within their areas.

The risks generated from the workshops were ranked for impact, probability, and catalogued into a database maintained and monitored by the ERM Division. The Department of Finance's "State Leadership Accountability Act Risks and Definitions" was used to categorize enterprise-wide risks.

The enterprise-wide risks were presented to the DMV Executive Leadership and the New Motor Vehicle Board in a series of meetings to identify the unit monitors and to determine the highest risks and mitigating controls. Once the highest risks were identified, DMV Internal Audits Staff met with the unit monitor for each risk to test mitigating controls.

EVALUATION OF RISKS AND CONTROLS

Operations- Internal- Technology—Outdated, Incompatible

DMV needs to fully modernize the legacy systems and replace its aged and outdated technology with broadly supported industry standard technologies. Systems have technical limitations and contain embedded business logic written in obsolete and antiquated programming languages. Significant resources are devoted to maintaining, managing, integrating and bridging aged systems with newer systems.

Controls:

Legacy System Integration: DMV has completed an independent assessment of the legacy systems, and is developing an action plan based on these findings. The DMV has integrated the legacy systems in such a manner that it functions with current and emerging technology. This method provides the DMV staff with ample time to adequately plan the retirement of legacy systems while actively operating and validating current technology. This integration does have a demonstrable cost, as the DMV must operate legacy systems, current systems, and bridge systems to allow integration between the legacy and current systems. Legacy integration is a stopgap method of extending the life of legacy systems that is performing as expected, and with the level of effort anticipated. By extending the life and functionality of the legacy systems, the DMV has mitigated the risk of the legacy systems becoming obsolete before it can be safely and properly retired.

Governance, Policies and Procedures: DMV controls the technology life-cycle through an effective governance program and standardization. The comprehensive governance model includes an overarching Enterprise Governance Council (EGC) to manage risk at the executive level. DMV's software management structure includes a Desktop Standards Committee to ensure desktop products are appropriate and supported. DMV's Enterprise Architecture program helps future-proof DMV's technology. An Architectural Review Board of DMV technical experts review enterprise technology prior to EGC consideration. DMV maintains written policies and procedures accessible to staff. The Patch and Vulnerability Management Group of technical experts is tasked with ensuring the security and integrity of DMV systems by implementing and managing all patching – abating or accepting risk with DMV systems. DMV conducts monthly technical meetings charged with similar functions, such as issue discussions, concerns, and future retirement plans for outdated systems. DMV effectively mitigates the risk of outdated technology by continuously managing the security, planning, and operation of the environment, and by documenting policies and procedures for all systems.

System Monitoring: The DMV utilizes multiple monitoring and logging systems to act as a

security tool and as a method of validating the functionality expected in all the DMV systems. To monitor the availability and sustainability of the DMV's systems, DMV uses real-time tools that enable the DMV to view system health. The DMV utilizes automated systems to report on system issues that require immediate intervention to manage. Administrative, system, and application information is logged to provide appropriate monitoring capabilities in the event of system issues. A comprehensive enterprise ticketing system for ensuring that data related to systems, inventory, history, and serial numbers are held in a repository for long-term use, and all changes are recorded for post-issue review. By utilizing multiple monitoring and logging systems and using information readily available to identify problems associated with outdated technology, the DMV mitigates the risk of technology being outdated.

Knowledge Transfer: The breadth of technology employed at the DMV coupled with staffing resources results in staffing with system specific knowledge. The DMV actively cross-trains personnel in areas where knowledge is system specific. In addition to actively managing human resources, the DMV documents systems that require specialized knowledge to maintain to address issues associated with attrition.

Operations- Internal- Staff—Key Person Dependence, Succession Planning

The aging workforce has made succession planning a top risk for DMV and the New Motor Vehicle Board (NMVB). Timely implementation on work products tend to necessitate that work be completed by the most experienced staff. This can result in less experienced staff not being afforded the opportunity to gain the needed experience and exposure, thus creating key person dependence.

Controls:

Governance and Training: Credited to a positive work environment, the DMV and NMVB staff are loyal employees with an immense amount of institutional knowledge. The DMV and the NMVB encourage upward mobility. The most experienced staff provides the new staff on-the-job training to fill in the gaps that traditional classroom training can't provide. The annual Individual Development Plan (IDP) prepares staff for upward mobility. Management uses the IDPs to identify staff for upward mobility opportunities which will serve to mitigate the loss of knowledge. For 2014, the DMV completed close to 100% of IDPs for all staff. The DMV has a robust training branch that offers a variety of program and state specific classes. Formal training programs are in place for most divisions. Other divisions schedule regular training workshops. Additionally, the DMV has a Leadership Development Academy developed exclusively for DMV by UC Davis Extension consisting of four programs that provides DMV executives, managers, supervisors, and non-supervisory staff an opportunity to obtain the knowledge, skills, and tools needed to perform their jobs with increased competency and efficiency and prepare them for upward mobility.

Retirement Monitoring: To assist DMV management in planning for retirements and ensure knowledge transfer, the DMV identifies the average age of DMV's major classifications on an annual basis. Management uses the information to plan and develop methods of knowledge transfer. The information can also be used to assist in recruitment efforts.

Policies and Procedures: Management identifies critical areas of key-person dependency and documents processes or ensures processes are updated and back-up analysts are trained. DMV and NMVB maintain comprehensive written policies and procedures for statutory functions. The written policies and procedures are easily accessible to staff and are reviewed and updated regularly.

Operations- External- Technology—Data Security

The DMV is responsible for the protection of data including personally identifiable information (PII). To ensure the privacy and security laws are followed, the DMV takes a proactive approach. The DMV data is valuable and has been a target for hackers; thus data security is a top risk.

Controls:

Network Security: The DMV ensures network level data protection through a stringent network protection methodology, practicing defense across the entire DMV domain. There are protection mechanisms preventing attacks including various intrusion systems, firewalls, and monitoring systems. The DMV utilizes defined network access mechanism with authentication mechanisms, to ensure data held within the DMV systems are accessed by authorized users that have been successfully authenticated. All accesses including successes and failures are logged to ensure availability of forensic information. By utilizing multiple levels of security to protect the network, the DMV mitigates the possibility of data being compromised.

System Security: The DMV provides protection for systems through various mechanisms contained within and external to systems. The DMV desktop systems utilize a host-intrusion protection system for thwarting threats that may enter through user action and couples this with external systems that perform filtering at the border to prevent access to internal systems via URLs or from received malware. We also practice internal Intrusion Detection Systems/Intrusion Prevention Systems for systems attached to DMV network resources. The DMV employs email scanning and containment for ensuring that the DMV data is protected from exfiltration. By utilizing multiple levels of security to protect the system, the DMV mitigates the possibility of data being compromised by user actions.

Security Operations Center (SOC): The SOC will monitor information from internal and external systems and networks for signs which may hold malicious intent, and take action as appropriate. The SOC will accept and consolidate input from all information streams for real-time monitoring and action. The SOC will be a consolidated unit providing the first line of defense for protecting critical information systems.

ONGOING MONITORING

Through our ongoing monitoring processes, the Department of Motor Vehicles reviews, evaluates, and improves our systems of internal controls and monitoring processes. As such, we have determined we comply with California Government Code sections 13400-13407.

Roles and Responsibilities

As the head of Department of Motor Vehicles, Jean Shiomoto, Director, is responsible for the overall establishment and maintenance of the internal control system. We have identified Bernard Soriano, Deputy Director, as our designated agency monitor(s).

Frequency of Monitoring Activities

The DMV is committed to ongoing monitoring and has tasked the Enterprise Risk Management (ERM) Division with the responsibility for the routine performance of department wide risk assessments. The ERM ongoing monitoring framework is modeled using the Department of Finance State Leadership Accountability Act lifecycle. Through a series of workshops with management and staff, risks and related controls are identified, assessed and documented. A risk register is developed and monitored monthly and updated as needed. Risks of concern are presented by the Agency Monitor to the Agency Head on a monthly basis. These risks and the associated control activities are monitored regularly.

Reporting and Documenting Monitoring Activities

The ERM Division’s Risk Management Office (RMO) is responsible for documenting and monitoring risks and controls captured within the risk register. Working through all levels of departmental personnel the RMO effectively rates these risks based on impact, likelihood and control effectiveness to determine a risk rating. The RMO prepares reports containing risk data on both risks that are considered enterprise in nature as well as divisional. These reports are shared with the Agency Head, Agency Monitor and

Deputy Directors.

Procedure for Addressing Identified Internal Control Deficiencies

If it is determined that control effectiveness is insufficient, the RMO reports such findings to the Agency Monitor who directs management to identify or develop additional controls. The RMO documents and monitors these newly identified or developed controls and reports progress to the Agency Monitor.

CONCLUSION

The Department of Motor Vehicles strives to reduce the risks inherent in our work through ongoing monitoring. The Department of Motor Vehicles accepts the responsibility to continuously improve by addressing newly recognized risks and revising risk mitigation strategies. I certify our systems of internal control and monitoring processes are adequate to identify and address material inadequacies or material weaknesses facing the organization.

Jean Shiomoto, Director
Department of Motor Vehicles

cc: Department of Finance
Legislature
State Auditor
State Library
State Controller
Secretary of Government Operations