December 22, 2015

Michael Cohen, Director
California Department of Finance
915 L Street
Sacramento, CA 95814

Dear Mr. Cohen,

In accordance with the State Leadership Accountability Act (SLAA), the Department of Justice 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 Tammy Lopes, Director, at (916) 324-4404, tammy.lopes@doj.ca.gov.

BACKGROUND

In California, the Office of Attorney General was created in 1850 to contend with what was considered at the time an unstructured, inadequate and inconsistent system of law enforcement.
Under the State Constitution, the Attorney General is elected on a statewide basis to serve as the chief law officer of California. It is the duty of the Attorney General to see that the laws of the state are uniformly and adequately enforced (Cal. Const., art.V, §13). The Attorney General manages and directs the Department of Justice (DOJ) and its law enforcement work, serves as legal counsel to state agencies, represents the state before the California and U.S. appellate and Supreme Courts, and issues formal opinions on the meaning of state law. The DOJ is the legal, administrative and law enforcement arm of the Attorney General. The department consists of seven divisions including Civil Law, Criminal Law, Public Rights, Law Enforcement, California Justice Information Services, Executive, and Administrative Support.

MISSION/GOALS

The Attorney General and department employees provide leadership, information and education in partnership with state and local governments and the People of California to:

- Enforce and apply all our laws fairly and impartially.
- Ensure justice, safety, and liberty for everyone.
- Encourage economic prosperity, equal opportunity and tolerance.
- Safeguard California's human, natural, and financial resources for this and future generations.

CRITICAL BUSINESS FUNCTIONS, OBJECTIVES, AND ACTIVITIES

The Attorney General represents the people of California in civil and criminal matters before trial courts, appellate courts and the Supreme courts of California and the United States by providing expert and efficient legal services. The Attorney General also serves as legal counsel to state officers and, with few exceptions, to state agencies, boards and commissions. Exceptions to the centralized legal work done on behalf of the state are listed in Section 11041 of the Government Code.

The Attorney General also assists district attorneys, local law enforcement, and federal and international criminal justice agencies in the administration of justice. To support California’s law enforcement community, the Attorney General coordinates statewide narcotics enforcement efforts, participates in criminal investigations and provides forensic science services, identification and information services and telecommunication support.

In addition, the Attorney General establishes and operates projects and programs to protect Californians from fraudulent, unfair, and illegal activities that victimize consumers or threaten public safety. The Attorney General also enforces laws that safeguard the environment and natural resources.

RISK ASSESSMENT PROCESS

In conducting its risk assessment, the DOJ used the July 2015 edition of the Ongoing Monitoring General Framework and Guidelines , published by the California Department of Finance's (DOF) Office of State Audits and Evaluations. The review is a continuous monitoring of operational processes to ensure the: (1) safeguarding of assets; (2) economical and efficient operations; (3) reliability and integrity of information systems; and (4) compliance with governing laws, rules and policies.

To monitor risk, DOJ management throughout the organization discuss existing and potential departmental risks at their weekly/monthly management meetings. Risk mitigation includes reviewing and updating departmental policies and procedures and changing or establishing processes.

In addition, the DOJ conducted a department-wide risk assessment. This risk assessment identified and evaluated threats and/or risks that could impede the DOJ's achievement of its mission, goals and objectives. The overall methodology included the development of an assessment evaluation tool that was distributed to the division directors and various levels of management within each DOJ division to identify their organizational activities, business processes and practices, and information and data that are critical to their mission, goals and objectives.

Initially each division's risk assessment was reviewed and analyzed by the Office of Program Review and Audits (OPRA). The OPRA focused its review on high risk areas for potential loss of agency assets and information. The OPRA then consulted with division directors and division management to discuss risks identified and the steps being taken, or that will be taken, to mitigate those risks.

All risks identified by division management through the risk assessment tool, including the high risk issues identified by OPRA, were presented to the DOJ Designated Monitors (DM) for consideration, evaluation and monitoring. Issues of lesser risk will continue to be monitored by division management and corrective actions will be taken in order to mitigate those risks.

A follow-up evaluation of internal control was conducted by OPRA and, where appropriate, recommendations were made to address risk and control issues identified. Issues and recommendations did not necessarily constitute control deficiencies but rather were enhancements to activities designed to achieve the DOJ's mission and goals.

EVALUATION OF RISKS AND CONTROLS

Operations- Internal- FI$Cal Conversion

Financial Information System for California (FI$Cal) Project

TheAccounting Information System (AIS) is a highly customized automatedaccounting information system that was developed by the DOJ in 1980. The AIS was designed with COBOL using indexed and sequential files. Because COBOL is an older platform being phased out in favor of newer platforms, recruiting qualified programmers with the background, skills, knowledge and abilities required to program and maintain the AIS has become increasingly difficult. The lack of available staff resources in conjunction with the critical information maintained in the AIS creates a high level of risk in the areas of information availability, accuracy of information, transparency of information, staff training, and access controlprivileges. As a result of issues regarding AIS, the DOJ has been participating as a Wave 4 department in the FI$Cal project in order to address the need for a new accounting system.

Risk #1:

In January 2015, the California State Auditor (CSA) raised concerns regarding the FI$Cal project and continues to identify the project as high risk. These concerns could result in a reduction in scope of the FI$Cal project and/or delays which will likely have an adverse impact on implementing of Wave 4 departments, such as the DOJ. The DOJ could face the following risks:

- The DOJ may be unable to find programmers with the COBOL skills needed to program and maintain the AIS to ensure it functions properly if the FI$Cal project is delayed. If the AIS failed to function properly and could not be repaired, the DOJ would be at risk of not producing its AIS outputs, such as billing, collections, reporting etc., which would adversely impact the department's ability to collect revenue and promptly pay department expenditures.
- Delays in the project could create high levels of risk in the areas of availability of information, accuracy of information, transparency of information, staff training, and access control privileges.

The DOJ will continue to participate as a Wave 4 department. The DOJ will continue to identify internal resources and available skilled information technology staff to assist the FI$Cal project with data management project tasks.

The DOJ continues to identify and document internal systems and subsystems that will interface and/or will be replaced with FI$Cal system to ensure that mandated data is captured, documented and properly retained.

Operations- Internal- Technology—Data Security

The DOJ collects and maintains data that includes public, confidential, personal and sensitive information that are important DOJ information assets. As part of protecting its information assets, the DOJ strives to manage data security and privacy by implementing appropriate security technologies, as well as develop and implement security policies, standards, guidelines, processes, and procedures.

Risk #2
In the event that there is unauthorized use, access, modification, loss, destruction, or disclosure of information assets, the following negative impacts to the DOJ could result:

- Impede the ability of DOJ employees to conduct their daily duties and prepare work products in order to meet deadlines that fulfill the DOJ’s mission, goals and objectives.
- Liability to State of California for failure to investigate and/or litigate cases resulting in civil penalties and judgments being assessed against state agencies and their employees.
- Possible sanctions or penalties by the court if the DOJ is unable to meet court mandated deadlines and requests for information.
- Possible civil action against the DOJ for failure to maintain a record concerning an individual if the result of such failure is determined to have had an adverse affect to the individual.
- Negative publicity that may occur in the aftermath of a breach of data or information.
- Increase in the risk to safety of officers who depend upon information availability and integrity for their daily operations to protect the public.

To mitigate this risk, the DOJ Information Security Office will work closely, on an ongoing basis, with the DOJ’s Network Information Security Unit to:

- Continue to revise and develop security policies, standards, guidelines, processes, procedures, and best practices, to further strengthen the DOJ security program to protect information assets.
- Identify, assess, and respond to the risks associated with information assets.
- Oversee the DOJ’s compliance with policies and procedures regarding the security of information assets.

- Continue to monitor computer equipment and servers for viruses and other security breaches on an ongoing basis.
- Continue to install patches and updates as necessary to safeguard against potential viruses and other security breaches.
- Ensure that programs that maintain confidential, sensitive and personal information follow standard operating procedures that are disseminated to staff in order to safeguard information assets.
- Revise and develop IT-related forms for authorized DOJ computer users.
- Ensure that all DOJ employees, vendors and contractors receive annual information security and privacy training.
- Continue to adapt to new security technologies to address new areas of concern.

Operations- External- FI$Cal Conversion

Financial Information System for California (FI$Cal) Project

Risk #3:
In January 2015, the CSA raised the following concerns regarding the FI$Cal project and continues to identify the project as high risk:

- CSA's IT expert is concerned that the apparent lack of opportunity for the executive working group to review progress and project issues as a body at a strategic level, particularly for a project that has been actively encountering schedule and resource issues.
- The California Department of Technology (CalTech) has provided Independent Project Oversight (IPO) to the FI$Cal project since 2009. However, continued turnover of the IPO staff assigned to the project has limited the ability of CalTech to provide timely analytical project reports to the Legislature, external oversight agencies, and other stakeholders.
- The Independent Verification and Validation (IV&V contractor continues to report concerns and make recommendations to the project, some of which the project has addressed, while other concerns have remained outstanding.
- In October 2014, the IV&Vreported that the project faces ongoing and increasing schedule and resource challenges that it did not anticipate. The challenges that the IV&Vnoted included the delayed and ongoing design, development, and testing activities for Wave 1 and concerns about the magnitude of software upgrades planned for Wave 3. According to the IV&V these challenges in tandem with the work associated with Waves 2 and 3, cannot be successfully met without substantial modification to the project's overall schedule.

In risk #1 in our SLAA report, we stated that the concerns CSA identified with the FI$Cal project could create "high levels of risk in the areas of availability of information, accuracy of information, transparency of information, staff training, and access control privileges". FI$Cal would ultimately lead to a new accounting system for DOJ that would replace the current antiquated DOJ "Accounting Information System" (AIS). The longer delays drag on in the development and completion of the FI$Cal project, the higher the risk to DOJ and other agencies who may also have accounting systems that need to be replaced. In addition, we identified in risk #1 the "internal operations risk" for DOJ; this would also extend to an "external operations risk", as accounting information from DOJ would also be used and relied upon by other State agencies outside of DOJ and also by agencies outside of the State.

Current DOJ FI$Cal implementation plan is a phased approach, with the Budget portion going live in 2015 (2015-16 FY), Procurement portion scheduled for July, 2016 (2016-17 FY), and full Accounting implementation scheduled for July, 2017 (2017-18 FY). DOJ has and will continue its on-going involvement in FI$Cal by actively contributing ideas and feedback to the FI$Cal team. Our hope is that through our active participation in the project and the DOJ staff that are currently dedicated to the project and working directly with FI$Cal project staff, that these additional resources will help fill some of the gaps identified as ongoing vacancy issues at FI$Cal. DOJ is committed to the success of the project not only as it benefits the DOJ and other state agencies but also to provide the people of California with transparent information as a result of the successful implementation of the FI$Cal project.

Operations- External- Technology—Data Security

Risk #4:
In the event that there is unauthorized use, access, modification, loss, destruction, or disclosure of information assets, the following negative impacts could result:

- Impede the ability of DOJ employees to conduct their daily duties and prepare work products in order to meet client deadlines.
- Liability to State of California for failure to investigate and/or litigate cases resulting in civil penalties and judgments being assessed against state agencies and their employees paid for by taxpayer money.
- Possible sanctions or penalties by the court if the DOJ is unable to meet court mandated deadlines and requests for information paid for by taxpayer money.
- Possible civil action against the DOJ for failure to maintain a record concerning an individual if the result of such failure is determined to have had an adverse affect to the individual.
- Increase in the risk to safety of officers who depend upon information availability and integrity for their daily operations in order to protect the public.

To mitigate this risk, the DOJ Information Security Office will work closely, on an ongoing basis, with the DOJ's Network Information Security Unit to:

- Continue to revise and develop security policies, standards, guidelines, processes, procedures, and best practices, to further strengthen the DOJ security program to protect information assets.
- Identify, assess, and respond to the risks associated with information assets.
- Continue to monitor computer equipment and servers for viruses and other security breaches on an ongoing basis.
- Continue to install patches and updates as necessary to safeguard against potential viruses and other security breaches.
- Continue to adapt to new security technologies to address new areas of concern.

ONGOING MONITORING

Through our ongoing monitoring processes, the Department of Justice reviews, evaluates, and improves our systems of internal controls and monitoring processes. The Department of Justice is in the process of formalizing and documenting our ongoing monitoring and as such, we have determined we partially comply with California Government Code sections 13400-13407.

Roles and Responsibilities

As the head of Department of Justice, Kamala Harris, Attorney General, is responsible for the overall establishment and maintenance of the internal control system. We have identified Tammy Lopes, Director, Victoria Sawyer, Special Assistant to the Chief Deputy Attorney General, as our designated agency monitor(s).

Frequency of Monitoring Activities

DAILY/WEEKLY/MONTHLY
- DOJ Executive management meet weekly to discuss issues facing DOJ.
- Management throughout DOJ meet to discuss existing and potential risks.
- DMs meet with the Executiveteam weekly and with DOJ management as-needed to discuss DOJ policies and procedures and address risks.

SEMI-ANNUALLY
- DMs provide updates to DOF on the status of risks through the DOF Corrective Action Plan process.

BIENNIALLY

- DOJ conducts a risk assessment every two years that utilizes an assessment evaluation tool. The risk assessment identifies and evaluates threats/risks that could impede DOJ's achievement of itsmission, goals and objectives.

ONGOING

- DMs evaluate the threats/risks that could impede DOJ's achievement of its mission, goals and objectives identified in the risk assessment.
- DMs utilize the results of reviews performed by OPRAand discuss with management the need to improve internal controls through updates to policies and procedures.
- Executivemanagement and the DMs are notified by OPRA concerning audits performed by state and federal audit agencies.
- DMs attend most entrance andexit conferences for audits performed.
- DMs assist in preparing audit responses to audit findings/recommendations to be submitted to the audit agency.

Reporting and Documenting Monitoring Activities

DOJ will issue Department-wide emails, memorandum, and administrative bulletins which communicate and detail Departmental policies and procedures related to control processes and means of documenting and monitoring various control processes.

DOJ ensures staff receive information vital to the effectiveness and efficiency of controls by encouraging management to update their teams through periodic meetings, both with individual staff and team staff as a whole. Minutes and/or notes related to meetings are maintained. In addition, DOJ encourages staff to discuss and consult with management if they discover issues that should be addressed to assist DOJ in fulfilling its mission, goals and objectives.

OPRA documents various control and monitoring systems and performs testing of these systems with workpapers documenting all work performed. Results of testing are communicated to DOJ management both in meetings and in written audit reports.

Procedure for Addressing Identified Internal Control Deficiencies

- DMs address deficiencies identified and evaluate the risk associated with each deficiency which are prioritized and steps are identified to mitigate and/or eliminate the risk.
- Risk mitigation may include reviewing and updating departmental policies and procedures in order to address risks identified.
- DMs attend most entrance and exit conferences for audits performed by state and federal agencies and actively participate in addressing weaknesses in internal controls as well as other deficiencies identified.
- DMs at a minimum are copied on all responses to audit findings/recommendationsand actively assist in preparing audit responses prior to submission to the audit agency.
- DMs participate in the DOF Corrective Action Plan updates for the SLAA report process by following up with staff responsible for addressing weaknesses previously identified.
- DMs meet with OPRA to discuss the results of internal control evaluations performed throughout the DOJ enabling them to update policies and procedures to address deficiencies.
- Updates to policies and procedures are communicated by email to all DOJ staff via Administrative Bulletins issued by the Director of the Division of Administrative Support.

CONCLUSION

The Department of Justice strives to reduce the risks inherent in our work through ongoing monitoring. The Department of Justice 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.

Kamala Harris, Attorney General

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