Memorandum

To: Marybel Batjer, Secretary
California Government Operations Agency

From: Amy Tong, Director
California Department of Technology

Date: December 26, 2017

Subject: STATE LEADERSHIP ACCOUNTABILITY ACT REPORT - 2017

In accordance with the State Leadership Accountability Act (SLAA), the California Department of Technology (CDT) submits this report on the review of our systems of internal control and monitoring process for the biennial period ending December 31, 2017.

Should you have any questions, please contact Randy Fong, Chief, Internal Audits, at (916) 403-9636 or via email at randy.fong@state.ca.gov.

Attachment

cc: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director, California Department of Finance
December 27, 2017

Marybel Batjer, Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Ms. Marybel Batjer,

In accordance with the State Leadership Accountability Act (SLAA), the Department of Technology submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2017.

Should you have any questions please contact Randy Fong, Internal Audit Manager, at (916) 403-9636, Randy.fong@state.ca.gov.

BACKGROUND

The mission of CDT and the State’s Information Technology (IT) community is to support state programs and departments in the delivery of state services and information to constituents and businesses through agile, cost-effective, innovative, reliable and secure technology.

Although the CDT receives 2 percent of its funding from the General Fund, the Department primarily operates as an Internal Service Fund organization (fee for service) and is responsible for California’s information technology portfolio including:

- Resources
- Project approval and oversight
- Strategic vision and planning
- Project management
- Enterprise architecture
- Data center and other IT services
- IT Policy
- Statewide Technology Procurements
- Training
- Security Policy and Oversight

The 2020 Statewide IT Strategic Plan included three strategic goals:

- Goal 1: Create One Digital Government
- Goal 2: Ensure Secure Delivery
- Goal 3: Build a Dynamic Workforce
With these goals, the CDT’s focus remains on realizing an enterprise approach to technology in order to effectively deliver public services and advance the public’s priorities, realize operating efficiencies, and enhance agility, reliability, and security.

The CDT is organized along two main areas of responsibility: one focused on the delivery of technology services and the other focused on technology policy and oversight.

**ONGOING MONITORING**

As the head of Department of Technology, Amy Tong, Director, is responsible for the overall establishment and maintenance of the internal control and monitoring systems.

**Executive Monitoring Sponsor(s)**

The executive monitoring sponsor responsibilities include facilitating and verifying that the Department of Technology internal control monitoring practices are implemented and functioning as intended. The responsibilities as the executive monitoring sponsor(s) have been given to: Chris Stevens, Chief Counsel, and Miles Burnett, Deputy Director, Administration Division.

**Monitoring Activities**

The department encourages on-going monitoring of its operations, including implementing external reports’ recommendations on high risk areas. Some of the recent reviews/assessments include: California State Auditor’s Reports No. 2014-062 (High Risk Update-Information Technology Oversight) and 2015-611 (High Risk Update-Information Security), August 2015. California State Auditor’s Report No. 2016-124 on CDT’s IT Procurement Division Oversight of the Competitive Bidding Process, June 2017. Department of General Services’ compliance audit of CDT’s Delegated Purchasing Program, August 2017. Annual Financial Audit of the Technology Service Revolving Fund conducted by MGO Certified Public Accountants, September 2017. Biennial Business Continuity Risk and Physical Vulnerability Assessment conducted by Aanko Technologies Inc., July 2016. In addition, the department has conducted on-going quarterly divisional rotational monitoring activities. The Administrative Services Division was the first division to conduct its self-monitoring activities, which began December 15, 2015. After the Administrative Division completed its quarterly monitoring report, our internal Information Technology Services division provided the results of its self-assessment review. Other divisions followed, and all high risk divisions had completed their self-assessment and reported to senior management by the biennial reporting period ending December 2017.

**Addressing Vulnerabilities**

The resulting final divisional monitoring activity report and corrective action plan, are discussed at on-going future semi-weekly executive staff meetings. Copies of the report and a corrective action plan will be disseminated to all division chiefs, including to the Chief, Internal Audits.

**Communication**

Each divisional corrective action plan will be documented in a format similar to the Department of Finance’s corrective action plan. Each division report and corrective action plan will be placed in a centralized on-line reporting depository accessible by department management personnel. Each corrective action plan will include follow-up semi-annual reporting by staff responsible to the division chief, and to the Chief, Internal Audits. All Internal control deficiencies reported on the corrective action plans will remain open until they are fully mitigated.
During periodic executive staff meetings, involving all deputy directors and key division chiefs, the department’s executive SLAA monitoring sponsors or delegated staff will present an update status of each open corrective action item. In addition, the current status of each corrective action is posted on the department’s internal Sharepoint site accessible to all CDT staff for viewing.

**Ongoing Monitoring Compliance**

The Department of Technology has implemented and documented the ongoing monitoring processes as outlined in the monitoring requirements of California Government Code sections 13400-13407. These processes include reviews, evaluations, and improvements to the Department of Technology systems of controls and monitoring.

---

**Risk Assessment Process**

The following personnel were involved in the Department of Technology risk assessment process: Executive Management, Middle Management, Front Line Management, and Staff.

**Risk Identification**

The CDT performed a department-wide risk assessment to gain an understanding of the department’s critical functions and objectives. The methodology undertaken to perform the risk assessment consisted of each department division performing a self-assessment of its operations and identify risk areas. The assessment focused on obtaining input regarding new risk areas that could hinder the department in meeting its mission and objectives. The assessment focused on business function processes and procedures, as well as administrative compliance issues that could pose high risks for the department.

In addition, management evaluated the results of recent audits conducted by the California State Auditor.

**Risk Ranking**

Each risk was evaluated on its potential impact and likelihood of occurring. A 5-point scoring system was used to measure each risk for potential impact and likelihood of occurring. A risk could receive a maximum score of 25. Risks considered high were further evaluated by senior management. The department’s chief internal auditor served as a coordinator to facilitate the risk assessment process and ensured management was provided with SLAA information and risk assessment procedures.

---

**Risks and Controls**


Customer migration from On-Premise Managed Services to Cloud technology will result in requiring changes to the way CDT operates this service area.

With the increasing popularity, CDT information technology customers are switching to Cloud services.

As a result staffing and equipment resources in our existing On-Premises Managed Services are at risk of being underutilized.
CONTROL A
CDT has developed teams to begin identifying the issues with resource allocations. Furthermore, CDT will need to develop a comprehensive work plan to address the issues identified and implement corrective actions.

RISK: COMPLIANCE-EXTERNAL-FUNDING—SOURCES, LEVELS
As a new audit program, resources are limited and may risk the Office of Information Security’s ability to conduct audits of all agencies.

As set forth in Government Code Section 11549.3, state entities shall comply with the information security and privacy policies, standards and procedures issued by the Office of Information Security (OIS). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the OIS, state entities shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. The OIS is responsible for overseeing compliance of state agencies to ensure implementation of requisite controls.

The OIS has implemented a new audit program to meet increased oversight expectations.

CONTROL A
CDT is working to develop a formal action plan by June 2018, which will address mitigating this risk. The plan should include addressing those state departments/agencies at most risk as priority information security audits. In addition, OIS will examine shortening the current audit lifecycle process from 6-9 months to a shorter time frame.

CONCLUSION
The Department of Technology strives to reduce the risks inherent in our work and accepts the responsibility to continuously improve by addressing newly recognized risks and revising controls to prevent those risks from happening. I certify our internal control and monitoring systems are adequate to identify and address current and potential risks facing the organization.

Amy Tong, Director

CC: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director of California Department of Finance
Secretary of California Government Operations Agency