

Department of Technology

2015 SLAA REPORT

December 31, 2015

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

Dear Ms. Batjer,

In accordance with the State Leadership Accountability Act (SLAA), the Department of Technology 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 Randy Fong, Internal Audit Manager, at (916) 403-9636, Randy.fong@state.ca.gov.

BACKGROUND

The mission of California Department of Technology (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 2015 Statewide IT Strategic Plan included six strategic goals:

- Goal 1: Responsive, Accessible and Mobile Government
- Goal 2: Leadership and Collaboration
- Goal 3: Efficient and Reliable Infrastructure and Services
- Goal 4: Secure Information
- Goal 5: Capable IT Workforce
- Goal 6: Responsive and Effective IT Project Procurement

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.

RISK ASSESSMENT PROCESS

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 a department-wide management survey requesting respondents to identify top risks within their areas of responsibility. A multi-divisional team of managers was formed to assess the results and validate the associated risks. 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.

Previous areas of moderate or low risks identified were evaluated with key management personnel to determine potential current impact. The assessment additionally 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 two recent audits conducted by the California State Auditor during 2015.

EVALUATION OF RISKS AND CONTROLS

Operations- Internal- Physical Resources—Maintenance, Upgrades, Replacements, Security

As of September 30, 2015, the CDT has \$256 million recorded in its equipment account. The recent completion of its triennial property inventory will reduce that amount by approximately \$57 million, which is a 22 percent reduction. This represents the value of over 560 assets that were disposed of over the last 10+ years without entering the disposal date in the fixed asset system. The primary contributing factor for this year's large reduction is that past year's inventory reconciliation procedures were not being fully followed. CDT has procedures in place that comply with the State Administrative Manual Section 8600 et. al., regarding property records procedures. These include the completion of property survey reports and delivery of discarded/surveyed equipment to General Services. However, the procedures for reducing the property inventory systems and the accounting records for traded-in-assets were not always followed.

CDT is currently developing a plan to place responsibility and accountability of equipment movement in each appropriate program area and to update its written procedures for timely reconciliations after taking each future equipment inventory.

Operations- Internal- Technology—Inadequate Support, Tools, Design, or Maintenance

As of September 30, 2015, the CDT has \$50 million recorded in its software account in its financial statement. Pursuant to CDT's Administrative Policy No. 1002, the department will conduct a 100% inventory of its software. Though certain areas of CDT have performed annually a software inventory for their responsible area, others have not. In addition, there is no uniform comprehensive record keeping of the department's software inventory, which can be reconciled to the software account in the financial statements.

CDT is currently working to develop a comprehensive work plan to complete conducting a 100% inventory of its software, and to reconcile to the software account in the financial statements.

Operations- External- Technology—Data Security

The CDT operates one of California's largest data centers that support state agencies' information technology needs. The data center is subject to thousands of hacking attempts every month. Given the State's increased use and reliance of information technology, CDT has a compelling need to ensure that it protects information assets, including its customers' data, information technology equipment, automated information, and software.

CDT continues to be diligent in its protection of the state's information assets by monitoring for anomalous activities, educating its workforce, and conducting assessments to identify and enhance its information security capability.

ONGOING MONITORING

Through our ongoing monitoring processes, the Department of Technology reviews, evaluates, and improves our systems of internal controls and monitoring processes. The Department of Technology 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 Technology, Carlos Ramos, Director, is responsible for the overall establishment and maintenance of the internal control system. We have identified Melissa Matsuura, Deputy Director, Administration Division, Tony Lewis, Chief Counsel, as our designated agency monitor(s).

Frequency of Monitoring Activities

The department encourages on-going monitoring of its operations. Some of the recent reviews/assessments include:

- Infrastructure Assessment Phase 1 Report conducted by KPMG, June 14, 2013
- Security Risk Assessment conducted by Performance Technology Partners, LLC, Dec. 2014
- Annual Financial Audit conducted by MGO Certified Public Accountants, June 2015
- State Personnel Board Compliance Review, August 2015

The department has planned to conduct on-going quarterly divisional rotational monitoring activities. The Administration Division is the first division to conduct its self-monitoring activities, which began December 15, 2015. The Administrative Division anticipates completing their monitoring activities and the reporting on their results by March 18, 2016. Lessons learned from this first divisional monitoring activity will help establish formal written departmental guidelines for other department divisions to conduct their monitoring activities and reporting. After the Administrative Division has completed its quarterly monitoring report, another division will begin its monitoring activities, and so forth.

Reporting and Documenting Monitoring Activities

The resulting final divisional monitoring activity report and corrective action plan, if any, will be discussed at the next subsequent monthly executive staff meeting. Copies of the report and a corrective action plan will be disseminated to all division chiefs, including to the Chief, Internal Audits.

Procedure for Addressing Identified Internal Control Deficiencies

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 responsible staff 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.

CONCLUSION

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

Carlos Ramos, Director

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