December 27, 2019

Julie Lee, Acting Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Ms. Julie Lee,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the Department of Technology submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2019.

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

GOVERNANCE

Mission and Strategic Plan

The California Department of Technology's (CDT) mission is to support the delivery of services to the people of California through secure, effective, and innovative technology solutions. The California Technology Strategic Plan (Vision 2020) includes the following goals and priorities:

- Goal 1: Create One Digital Government

- Increase operational agility and performance in the delivery of technology services
- Improve the design and delivery of digital services
- Foster collaboration and boundaryless behavior
- Transform and simplify the way government does business through innovation
- Accelerate the adoption of common technology platforms and share services

- Goal 2: Ensure Secure Delivery

- Protect California's information assets and maximize data access
- Develop a robust and collaborative security risk reduction strategy
- Develop an enterprise approach to security leadership and governance
- Improve and invest in security capabilities to protect mission-critical systems and data
- Foster a security-minded culture throughout California's workforce

- Goal 3: Build a Dynamic Workforce

- Create a culture of innovation and collaboration
- Develop the capabilities of both technology leaders and functional experts
- Improve employee engagement and increase retention of quality employees
- Expand our pool of skilled and experienced technology professionals
- Foster a diverse and unified technology community

With these goals, CDT developed a departmental roadmap to achieve Vision 2020. 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 Year One (2017) internal departmental roadmap sought to align CDT's business and technical services strategy into an integrated service delivery framework, provide greater strategic clarity and improve service delivery. The Year One Strategy included the following three Strategic Focus Areas and a North Star Goal to become "One CDT" with a shared identity and culture.

- Organization Sustainability

- To improve our reputation and make CDT more relevant on IT in the state of California.
- To move CDT toward greater capacity and sustainability.
- To grow, mature, and transform CDT's service offerings by taking the necessary steps to make them viable, sustainable, and aligned with customer needs.

- Statewide IT Project Delivery

    - To improve statewide IT project delivery and the planning, quality, value, and the likelihood of success of our customers' IT projects by strengthening CDT's statutory role of checks and balances – "guardrail services" – such as Project Approval Lifecycle, IT Procurement, and Project Oversight.

- Statewide Information Security

- To protect California's information assets by providing statewide leadership and collaborating with partner departments in information security.

The Year Two / Three (2018, 2019) roadmap brought departmental goals into further alignment with Vision 2020, including the following three Strategic Focus Areas and North Star Goal to "Model the Way".

- Strengthen Organizational Value

- Become an essential partner to the State of California by working together to minimize risk, increase the probability of project success, and achieve the desired outcomes of our customers through both guardrail and consultative services.

- Transform Service Delivery

- Transform how services are delivered through greater innovation and a commitment to digital service delivery in order to provide cost-effective, reliable, and secure technology services to the State of California.

- Foster Excellence and Accountability

- Foster a culture of excellence and accountability by enabling CDT's workforce to deliver quality services and innovative solutions to our customers with pride.

CDT has broad responsibility and authority to guide the application of information technology in California State Government. CDT's primary areas of responsibility include policymaking, interagency

coordination, IT budget and procurement review, technical assistance, and advocacy. CDT is responsible for policy and oversight of IT projects, information security, IT procurement, and providing general-purpose technology services to state entities. These responsibilities include the initiation, approval, implementation, management, oversight, and continuation of IT projects and allows CDT to review, approve, and provide oversight of any service contract that contains an IT component. CDT's Office of Technology Services is responsible for providing general-purpose technology services to meet the common technology needs of executive branch entities, eliminate duplications, and bring about economies of scale. CDT's Office of Information Security is responsible for establishing an information security and privacy program including policies, standards, and procedures; directing state agencies to effectively manage security and risk; reporting security and privacy incidents; disaster recovery planning; independent security assessments; and audits of information security program compliance.

Control Environment

CDT's management creates and demonstrates the importance of integrity and ethical values through its attitudes, behavior, and the verbal and written standards of conduct it establishes and communicates throughout the organization. CDT's management sets the tone for what is expected throughout the organization and reinforces the organization's commitment to doing what is right.

CDT's oversight structure consists of CDT's executive leadership team and several external advisory bodies that assist CDT in setting the state's strategic and operational direction. These external bodies include:

- Information Technology Executive Committee: Central governance and decision-making body comprised of executive leadership to oversee statewide technology strategy, policy, oversight, and service offerings. Attendees: CDT executive staff, AIOs and CIO liaisons from constitutional/independent entities, DOF and DGS.
- Technology Operations Advisory Council: Advisory customer- and service-focused body comprised of executive state leadership and local government technologists who provide customer-centered input on shared CDT service offerings, rates, and opportunities for cross-agency collaboration. Attendees: CDT executive staff, AIOs, Agency/Department technologists, local city/county CIOs.
- Information Security Advisory Council: Advisory security-focused body comprised of state security representatives to provide input and training on security policy, procedures, standards, guidelines. Attendees: Agency ISOs.
- Project Management Advisory Council: Advisory project delivery-focused body comprised of state project management professionals to provide input on project challenges, opportunities, shared services, standards and frameworks. Attendees: Agency/Department Project Management Leadership.
- Workforce Development Advisory Council: Advisory workforce-focused body comprised of executive leadership, training and HR representatives that provide input on workforce development initiatives. Attendees: CalHR, GovOps and select AIOs and CDT Office Chiefs.

CDT's organizational structure is determined by its executive leadership team, following state personnel guidelines which ensures that appropriate levels of responsibility and authority are instituted across the organization.

CDT maintains documentation of its control system through verbal and written communication,

including management oversight to ensure that operations run efficiently and effectively, written reports, and other documentation that produces reliable information about the organization's operations and its compliance with applicable laws and regulations.

CDT establishes, sustains, and retains a competent workforce by hiring competent staff, providing training opportunities to increase staff skill levels, mentoring staff to better align their skillset with the organization's objectives, and creating a positive work environment to motivate high performance and retention.

CDT enforces accountability from the top down, from the Directorate through executive staff to senior staff to entity personnel who are accountable for performing their assigned internal control responsibilities. Management holds personnel accountable through mechanisms such as routine oversight, annual performance appraisals, and disciplinary actions.

Information and Communication

CDT communicates information necessary to achieve its objectives through both internal and external channels. Internal channels include all-staff meetings, town hall meetings, executive leadership meetings, senior staff meetings, office leadership meetings with the Directorate, and managers and supervisors offsite meetings.

CDT's Executive Leadership Team also takes an active role in facilitating communication with CDT's various stakeholders. This includes several events, forums, conferences, and task forces that CDT leads or engages with to promote the state's vision and strategic direction, including the Information Technology Executive Committee, Technology Operations Advisory Council, Information Security Advisory Council, Project Management Advisory Council, Workforce Development Advisory Council, Technology Leadership Forum, CDT Customer Forum, Agency CIO Roundtable, Agency Portfolio Meeting, Information Security Officer Quarterly, Statewide Enterprise Architect Roundtable, Digital Web Services Network, and various Legislative Briefings.

CDT also engages private sector vendors and local government throughout the year to enhance the partnership with external stakeholders that represent national, local government, and vendor organization. These strategic partners serve a critical role in helping CDT deliver services to the citizens of California: California County Information Services Directors Association, Municipal Information Systems Association of California, Civic Advisory Council, Vendor Advisory Council, Vendor Partner Forum, Vendor Association Meetings, Strategic Vendor Meetings, and the National Association of State Chief Information Officers.

Relevant and reliable information is communicated and processed through these channels as well as through various written documents that CDT produces. CDT uses several information systems to record pertinent operational, programmatic, and financial information, including SharePoint, ServiceNow, and PeopleSoft.

MONITORING

The information included here discusses the entity-wide, continuous process to ensure internal control systems are working as intended. The role of the executive monitoring sponsor includes facilitating and verifying that the Department of Technology monitoring practices are implemented and functioning. The

responsibilities as the executive monitoring sponsor(s) have been given to:
Chris Stevens, Chief Counsel; and Miles Burnett, Deputy Director, Administration Division.

CDT ensures the effectiveness of its internal control systems through executive and senior management oversight, internal reviews, and external reviews. CDT executive and senior management oversight includes status meetings, review and discussion of relevant reports, and other monitoring activities. CDT holds weekly meetings at the executive level and bi-weekly meetings at the senior management level to discuss critical priorities, project status, and issues that need to be remediated and/or escalated. CDT's Directorate holds monthly meetings with Office Chiefs to discuss workforce planning, workload priorities, and the status of assigned initiatives.

Internal reviews include an internal audit function that routinely performs audits of CDT's internal controls. CDT's operations are also routinely audited by various external entities. Some of the recent audits/reviews/assessments include:

- California State Auditor's Report 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.
- California State Auditor's Report No. 2017-601 (High Risk – Updated Assessment of High-Risk Issues the State and Select State Agencies Face
- California State Auditor's Report No. 2019-601 (High Risk – Updated Assessment of High Risk Issues the State and Select State Agencies Face. Estimated Release Date: January 2020
- 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.
- Annual Financial Audit of the Technology Service Revolving Fund conducted by Brown Armstrong Accountancy Corp, September 2018.
- Annual Financial Audit of the Technology Service Revolving Fund conducted by Brown Armstrong Accountancy Corp, September 2019.
- Biennial Business Continuity Risk and Physical Vulnerability Assessment conducted by Aanko Technologies Inc., July 2016.
- Social Security Administration Compliance Review Report No. 201-CA.

CDT assigns responsibility for monitoring and addressing vulnerabilities identified through monitoring to the responsible executive under whose area the issue resides. Progress to reduce identified vulnerabilities is monitored through regular assessments by the responsible executive for that area and through quarterly reporting from CDT's internal auditor.

In addition, the resulting final divisional monitoring activity report and corrective action plan will be discussed at weekly executive staff meetings. Copies of the report and a corrective action plan will be disseminated to all division chiefs. 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 executive staff meetings, 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.

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.

The following methods were used to identify risks: brainstorming meetings, ongoing monitoring activities, audit/review results, and other.

The following criteria were used to rank risks: likelihood of occurrence, and potential impact to mission/goals/objectives.

CDT performed a department-wide risk assessment to gain an understanding of the department's critical functions and objectives. The method undertaken to perform the risk assessment consisted of each division performing a self-assessment of its operations to 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. 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.

RISKS AND CONTROLS

Risk: Cost Recovery Challenges

CDT faces different types of challenges ensuring that its costs can be effectively recovered.

- One cost recovery challenge pertains to the rapidly evolving technology landscape. Evolving technologies such as cloud services will impact CDT's mature service offerings as customers migrate to these technologies. As CDT's managed service customer base continues to decline due to customers migrating to external cloud services, CDT may not be able to reduce its fixed cost structure at the same pace as these migrations occur. Consequently, CDT could struggle to recoup investments in managed service infrastructure and staffing. Continuing to maintain high operating costs against a decreasing managed service customer base puts the department at risk of failing to generate sufficient revenue to cover its costs.
- Another cost recovery challenge pertains to CDT's project oversight role. Since oversight costs are built into project plans and funded as part of project costs, departments resist CDT's involvement.

Control: A. Reduce and Simplify

CDT is actively working on a plan to address under-recovering services and is pursuing more cost effective solutions to deliver services. These solution include leveraged cloud services, software defined networking, standardized architecture, and extending its on-premises managed services to the cloud. CDT will reduce and simplify its portfolio of services to focus on core competencies, strategic direction, and services that generate sufficient revenue to meet or exceed expenses. CDT is also pursuing alternatives to its current cost recovery funding model that encourages and enables effective oversight and innovation and decreases the pressure on CDT to delegate more projects.

Risk: Recruiting and Retaining Competent Staff

CDT faces the risk of losing critical knowledge, skills, and expertise required to provide quality data center and managed services, as well as IT procurement services. These losses are due to a significant number of upcoming retirements, challenges recruiting and retaining well qualified staff, and the difficulties of maintaining and updating staff skills to align with a continually evolving technology landscape.

Control: A. Identify, Prioritize, Improve, and Modernize

CDT will identify skill gaps based on strategic direction and identify business critical positions to develop prioritized training and knowledge transfer plans. It will improve and modernize recruitment and hiring practices using social media, and expand the use of non-traditional options (telework, alternate work week) to attract and retain a talented workforce. It will create and implement training plans and ensure a career ladder is in place

Control: B. Reduce and Redirect

CDT will reduce services currently under-utilized or under-recovering and focus on a core set of services to minimize the variety of skills needed to support CDT's service portfolio. It will redirect talent from lower value support functions to those that directly support business critical programs and services.

Risk: Out-of-Date Applications

Some of CDT's data center customers are using out-of-date applications due to the expense, business risk, and technical hurdles inherent with updating many of these systems. Running out-of-date applications requires increased staff support and poses increased security risks, service failures, legal liability, and support costs for critical IT systems:

- Security – Manufacturers typically stop providing standard support and fixes for known problems, including security patches. This security risk not only impacts this specific unsupported system, but could compromise the entire data center.
- Reliability – Risk of hardware outages increases significantly each year these applications are in service beyond life expectancy. Replacement parts are also harder to find, which can increase restoration time from days into weeks.
- Legally – The state can face heavier fines and/or legal actions if a data breech occurs on

outdated technologies.
- Cost – Additional support is needed to handle the more frequent outages and any other special handling needed.

Control: A. Software Updates

CDT will prioritize and actively work with customers to update their systems to current levels. For those customers that cannot or will not update their systems, CDT will determine the impact of supporting out-of-date software and start charging them a premium for using non-standard software versions.

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 risk mitigation strategies as appropriate. 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