December 14, 2023

Amy Tong, Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Secretary Amy Tong,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the California Department of Tax and Fee Administration submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2023.

Should you have any questions please contact Nicolas Maduros, Director, at (916) 309-8300, nick.maduros@cdtfa.ca.gov.

GOVERNANCE

Mission and Strategic Plan

The California Department of Tax and Fee Administration (CDTFA) administers California's sales and use, fuel, tobacco, alcohol, and cannabis taxes, as well as a variety of other taxes and fees that fund specific state programs. CDTFA administered programs collect over $94 billion annually which in turn supports local essential services such as transportation, public safety and health, libraries, schools, social services, and natural resource management programs through the distribution of tax dollars going directly to local communities.

CDTFA's Mission and Goals are as follows:

Mission: We make life better for Californians by fairly and efficiently collecting the revenue that supports our essential public services.

Goal 1: Modernize Tax Administration

Goal 2: Improve the Taxpayer Experience

Goal 3: Support Our Team

Control Environment

CDTFA's leadership is committed to honesty, integrity and ethical behavior. These values are central to CDTFA's control environment. Ethical concerns are reported through the Director's Comment Box, Employee Hotline, and State Whistleblower Hotline.

The Director oversees operations, while CDTFA leadership (senior staff) manage their program areas to establish an effective control environment.

CDTFA has adopted the "Three Lines of Defense" model, as outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This model allows the department to better establish and coordinate duties related to risk and control.

These three lines of defense consist of the following:

First Line- Operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks. This includes recruiting, developing, and maintaining a competent workforce; as well as, evaluating performance and enforcing accountability.

Second Line- Enterprise Risk Management Committee (ERMC), governance/steering committees, TSD's cybersecurity system, and other control functions monitor and facilitate the implementation of effective risk management and assist risk owners in reporting adequate risk related information throughout the department.

Third Line- The Internal Audit Bureau, through a risk-based approach to auditing and consulting services, provides assurance to the department's audit committee and senior staff that internal control systems are in place and documented. This assurance covers the effectiveness of the first and second lines of defense.

Information and Communication

Senior staff meets weekly to discuss operational and program issues within the organization. These meetings collect and communicate relevant information needed for decision making. In some cases, work groups report back to senior staff on various operational, program, and financial matters. Additionally, the Director and Chief Deputy Director regularly meet with deputy directors.

CDTFA communicates with team members across the enterprise through several channels:

- Senior staff members share information with their managers and supervisors through team meetings.
- CDTFA's Director frequently conducts all team member meetings, which are livestreamed throughout the department, and team members participate by asking questions via chat or email.
- External Affairs Division (EAD) prepares the CDTFA Express, a weekly electronic newsletter.
- CDTFA utilizes an intranet site (myCDTFA) to communicate current events and information.
- Internal campaigns utilize videos, posters, banners, and emails.
- Program areas conduct virtual and in-person training for their team members (e.g., Centralized Revenue Opportunity System (CROS), tax law, contracts, hiring processes, and attendance coordinator duties).
- Human Resources Bureau organizes and delivers quarterly new employee events.
- Administration Division conducts an employee engagement survey and coordinates the annual leadership conference.
- Team members use Microsoft Teams and SharePoint Online to work collaboratively on

assignments.

Channels for communicating and sharing information with external stakeholders include:

- CDTFA website
- Special notices
- Newsletters
- Social media
- Taxpayer workshops and seminars
- Interested parties meetings
- Annual Taxpayers' Bill of Rights meetings
- Open Data Portal
- Meetings with control agencies
- Tax Advisory / Tax Practitioner meetings
- Toll-Free 800 Number

CDTFA team members can report inefficiencies and inappropriate actions to management using the following methods:

- Meetings with managers and supervisors.
- Director's Comment Box found on myCDTFA intranet, which allows team members to submit suggestions, feedback, and comments to the Director.
- Employee Hotline allows all team members to report employee misconduct confidentially and without fear of reprisal. The Internal Affairs Section (IAS) investigates complaints and allegations involving violations of policies or laws related to CDTFA employees.
- Diversity and Inclusion Office handles concerns regarding sexual harassment, discrimination based on protected status; as well as retaliation related to an Equal Employment Opportunity complaint.
- Interviews with the Internal Audit Bureau during an audit review to determine if CDTFA's internal control processes are adequate and functioning.
- State Auditor Whistleblower Program, which allows team members to report employee misconduct and improper activities to the State Auditor.

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 California Department of Tax and Fee Administration monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to: Nicolas Maduros, Director.

The CDTFA's ERMC is comprised of the Director, Chief Deputy Director, Chief Counsel, Division Deputy Directors, and select Bureau Chiefs. CDTFA's Director is the chair of the ERMC and the other members are a part of the governing body. Internal Audit Bureau facilitates the meetings. The ERMC takes a risk-based approach to managing the department's risks and integrating concepts of internal control and strategic planning.

The ERMC team conducts a thorough assessment of the potential risks and vulnerabilities to the department. CDTFA's risk management strategy is to reasonably assure that significant risks to CDTFA are identified, prioritized, and managed on an ongoing basis to ensure the successful accomplishment of the organization's core workload and strategic goals and objectives.

In addition, CDTFA's Internal Audit Bureau provides auditing, consulting and risk management services while working with management to evaluate controls, identify risks, streamline processes, and provide sustainable recommendations.

RISK ASSESSMENT PROCESS

The following personnel were involved in the California Department of Tax and Fee Administration risk assessment process: executive management, middle management, front line management, and staff.

The following methods were used to identify risks: brainstorming meetings, employee engagement surveys, ongoing monitoring activities, audit/review results, other/prior risk assessments, external stakeholders, questionnaires, consideration of potential fraud, and performance metrics.

The following criteria were used to rank risks: likelihood of occurrence, potential impact to mission/goals/objectives, potential impact of remediation efforts, and tolerance level for the type of risk.

RISKS AND CONTROLS

Risk: Cybersecurity

The security of confidential data, as well as Personally Identifiable Information (PII) and other sensitive data, is critical to CDTFA's ongoing mission. A breach of confidential data within the CDTFA infrastructure, including the Centralized Revenue Opportunity System (CROS) and statewide Financial Information System for California (FI$Cal), may lead to the department's inability to effectively administer California's taxes and fees, revenue loss, and damage to CDTFA's reputation. Vulnerabilities and attacks, such as denial-of-service attacks, phishing, malware, and ransomware, of CDFTA systems could result in impacts to the confidentiality, integrity, and availability of CDTFA data and services.

Control: NIST Cyber Security Framework- Identify

CDTFA develops and implements an organizational understanding to manage risk to systems, assets, data, and capabilities. This includes the following activities:

- Identify critical enterprise processes and assets.
- Document information flows.
- Maintain hardware and software inventory.
- Establish policies for cybersecurity that include roles and responsibilities.
- Identify threats, vulnerabilities, and risk to assets.

Control: NIST Cybersecurity Framework- Protect

CDTFA develops and implements appropriate safeguards to ensure delivery of services. This includes the following activities:

- Manage access to assets and information.
- Protect sensitive data.
- Conduct regular backups.
- Secure and protect devices.
- Manage device vulnerabilities.
- Train users.
- Conduct phishing simulation exercises.

Control: NIST Cybersecurity Framework- Detect

CDTFA conducts detection processes to identify the occurrence of a cybersecurity event. This includes the following activities:

- Test and update detection processes.
- Maintain and monitor logs.
- Know the expected data flows for the enterprise.
- Understand the impact of cybersecurity events.

Control: NIST Cybersecurity Framework- Respond

CDTFA develops and implements the appropriate activities to take action regarding a detected cybersecurity event. This includes the following activities:

- Ensure response plans are tested and updated.
- Coordinate with internal and external stakeholders.

Control: NIST Cybersecurity Framework- Recover

CDTFA develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. This includes the following activities:

- Communicate with internal and external stakeholders.
- Ensure recovery plans are updated.
- Manage public relations and department reputation.

Risk: Team Member Safety

Due to CDTFA being a tax collection department and administering controversial tax and fees, there is an increased safety risk to CDTFA team members performing compliance, collection, audit, and enforcement activities that could result in physical threats.

Control: Headquarter Controls

CDTFA has several safeguards in progress at its headquarter office to keep team members safe. These include:

- Reviewing Badge access reports.
- Testing surveillance cameras.
- Testing audible alarm.
- Implementing redesigned badges.
- Conducting Business Management Bureau and CHP safety assessments.
- Planning emergency preparedness training.

CDTFA will continue to conduct regular, ongoing security reviews to ensure the systems, processes, and procedures are effective.

CDTFA headquarters will be moving to a new location in 2024 and will reassess the above controls to ensure safeguards are working as intended at the new building.

Control: Field Controls

CDTFA has safeguards in progress to help ensure team member safety while performing compliance, collection, audit, and enforcement activities in the field. These include:

- Reviewing contracts with law enforcement and a private transportation security company to determine the effectiveness and if further controls can be implemented.
- Assessing safety equipment needs for team members to use while in the field.
- Exploring additional training opportunities related to active shooter, de-escalation, and communication techniques when encountering difficult situations.
- Assessing the need for site safety assessments and ensuring adequate safety measures to prevent burglary, theft, and counterfeit currency at CDTFA locations.
- Monitoring and analyzing data access surrounding physical and facility security (e.g., alarm testing, badge access, and visitor badging).
- Identifying potential threats to CDTFA team members.

Risk: Workforce Changes and Modernization

Changes in the work environment and labor market are impacting CDTFA's ability to recruit, retain, develop, and maintain a stable workforce while preserving essential skills and critical knowledge.

Control: Recruitment and Retention Initiatives

CDTFA has several recruitment and retention initiatives in progress such as:

- Classification consolidation project.
- In-person hiring events.
- Student Assistant, Apprenticeship, & Intern Programs (through the Statewide Employment Initiative and other resources).
- Position rotation program.
- Training and Development (T&D) assignments.
- Wellness, affinity, and volunteer activites.
- You Make a Difference Campaign.
- Diversity & Inclusion Celebration Committee and events.

Control: Workforce and Succession Planning Initiatives

CDTFA is working on several workforce and succession planning initiatives, such as:

- CDTFA Workforce and Succession Plan.
- Leadership Development Program and training initiatives.
- Mentoring Program and Speed Mentoring Program.
- Job shadowing opportunities.
- Upward Mobility Program.

CONCLUSION

The California Department of Tax and Fee Administration 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.

Nicolas Maduros, Director

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