December 29, 2025

Nick Maduros, Secretary
California Government Operations Agency
1304 O Street, Suite 300
Sacramento, CA 95814

Dear Secretary Nick Maduros,

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, 2025.

Should you have any questions please contact Trista Gonzalez, Director, at (916) 309-8300, Trista.Gonzalez@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 $97 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) manages 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 (ATM) meetings and Touch Base meetings, which are livestreamed throughout the department. Team members can participate during ATM's by asking questions via chat or email.
- External Affairs Division (EAD) prepares the CDTFA Express, a weekly electronic newsletter, which includes important updates and highlights various CDTFA leaders and team members.
- EAD plans frequent Eat and Greet lunchtime sessions, where team members can

connect with CDTFA leadership in a casual setting.

- 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 orientation events.
- Administration Division conducts an employee engagement survey and coordinates leadership conferences throughout the year.
- 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: Trista Gonzalez, 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. As technology advances, the cyber threat landscape continues to evolve, introducing new potential threats and attack vectors. A breach of confidential data within the CDTFA infrastructure, including the Centralized Revenue Opportunity System (CROS), may lead to the department's inability to effectively administer California's taxes and fees, revenue loss, and damage to CDTFA's reputation. CDTFA aligns security practices with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to reduce risk and the likelihood of a cyber incident from disrupting CDTFA's ability to carry out its mission.

Control: NIST Cybersecurity Framework - Govern

CDTFA establishes strategies, policies, and oversight for cyber risk management in alignment with business objectives. This includes the following activities:

- Define and formalize the cybersecurity priorities, constraints, and risk tolerance/appetite statements; communicate and integrate them into operational risk decision-making processes.
- Develop, publish, and enforce policies aligned with business objectives and compliance requirements.
- Collect and analyze results from enterprise-wide cybersecurity risk

management activities to inform and adjust the overall risk management strategy.

Control: NIST Cybersecurity 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 information 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.
- Continuous monitoring.
- 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 communication with internal and external stakeholders.
- Conduct post-response lessons learned.

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:

- Ensure recovery plans are updated.
- Prioritize restoration of critical business functions.
- Communicate with internal and external stakeholders.
- Manage public relations and department reputation.

Risk: Team Member Safety

Due to CDTFA being a department that administers and collects various taxes, fees, and licenses, there is an increased safety risk to CDTFA team members performing compliance, collection, audit, and enforcement activities that could result in physical threats.

Control: Safety Measures

CDTFA has several safeguards in progress to help ensure team member safety, such as:

- Monitor and analyze data for physical access and review badge access reports.
- Conduct Business Management Bureau inspections and CHP safety assessments.
- Continue site and security safety assessments for burglaries, theft, counterfeit currencies, and evidence management.
- Plan emergency preparedness training and identify additional training opportunities and guidance for team members when encountering difficult situations.
- Plan department-wide safety events.
- Monitor contracts with law enforcement and a private transportation security company.
- Assess team members' safety equipment needs.
- Identify, monitor, and evaluate 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.
- Job shadowing and Training and Development (T&D) assignments.
- Wellness, affinity, volunteer, diversity and inclusion activities, and program 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.
- 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.

Trista Gonzalez, 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