December 17, 2021

Yolanda Richardson, Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Secretary Yolanda Richardson,

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, 2021.

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 $70 billion annually which 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 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 Collections to Adapt to the 21st Century Economy

Goal 2: Improve Taxpayer Services

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 programmatic 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, programmatic, and financial matters. Additionally, the Director and Chief Deputy Director regularly meet with deputy directors in bi-weekly meetings.

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 staff participate by asking questions in person, chat, or via email.
- External Affairs Division (EAD) prepares the CDTFA *Express*, a weekly electronic newsletter.
- EAD and Technology Services Division (TSD) developed an Intranet site (*my*CDTFA).
- Internal campaigns utilize posters, banners, and emails.
- Program areas conduct virtual training for their team members (i.e., Centralized Revenue Opportunity System (CROS), contract and hiring processes, attendance coordinator duties, etc.).
- Human Resources Bureau organizes new employee orientation.
- Administration Division conducts an annual employee engagement survey and coordinates leadership conferences.
- 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 Taxpayer Bill of Rights meetings
- Open Data Portal
- Meetings with control agencies

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 *my*CDTFA 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 takes measures to successfully reduce risks and vulnerabilities to a reasonable and appropriate level.

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.

External auditors and CDTFA Information Security Office also identify and address vulnerabilities by ensuring policies, procedures, standards and/or guidelines are effective. These vulnerabilities are monitored through reports and Corrective Action Plans (CAPs).

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: Pandemic Impact on Business Operations

The ongoing pandemic is impacting CDTFA's daily business operations by raising concerns about team member safety, collaboration, recruitment and retention, productivity and accountability, training, and employee morale.

Control: A. COVID-19 Safety Protocols

As a large department that serves the public, CDTFA team members are at risk of encountering people who may have COVID-19. To ensure team member safety, the CDTFA expanded it's telework program and serves the public by appointment in field offices.

CDTFA created a Return-to-Office Committee to develop and implement a plan to safely allow team members who have been teleworking full time to return to their respective offices 50% of the time. The plan also includes the statewide COVID-19 testing mandates for those team members who have not provided proof of vaccination or have declined to disclose their vaccination status.

Control: B. Adapting to a Hybrid Workforce

CDTFA has several initiatives to adapt to the hybrid workforce created by the pandemic. These initiatives include:

- Updating the department's current telework policy.
- Hosting virtual open houses and participating in recruitment fairs.
- Converting in-person training to virtual.
- Increasing communications through all team meetings, and weekly the Express newsletter.
- Conducting virtual speed mentoring sessions and new employee orientation.
- Emphasizing wellness through online resources, webinars, and applications (i.e., Healthier U).
- Utilizing Microsoft Teams to collaborate with peers in other offices, recruitments, mentoring, and special projects.

- Providing performance and labor relations training for supervisors and managers.

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.

CDTFA utilizes the NIST Cybersecurity Framework to manage and reduce information security risks. The framework consists of five key functions - Identify, Protect, Detect, Respond, Recover. These functions comprise the controls that will be in place to manage cybersecurity for the department.

Control: A. 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: B. 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.
- Securely protect devices.
- Manage device vulnerabilities.
- Train users.

Control: C. 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.
- Understanding the impact of cybersecurity events.

Control: D. 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.
- Ensure response plans are updated.
- Coordinate with internal and external stakeholders.

Control: E. 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, there is an increased safety risk to CDTFA team members performing compliance, collection, audit, and enforcement activities that could result in physical threats and/or harm.

Control: A. Headquarter Controls

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

- Reviewing Badge access reports
- Surveillance camera testing
- Audible alarm testing

With COVID restrictions in place and most of CDTFA team members teleworking, some headquarter controls were postponed. As team members return to the office, CDTFA will re-evaluate it's plans to implement:

- New Temporary Badging system for visitors
- Redesigned Badges
- Business Management Bureau (BMB) and CHP safety assessments

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

Control: B. Field Office Controls

Below are controls that help ensure Field Operations Division (FOD) team member safety while performing compliance, collection, audit, and enforcement activities. FOD has:

- Executed several contracts with law enforcement and a private transportation security company to ensure the safety and protection of team members while performing core functions.
- Purchased safety equipment (i.e., masks, protective & safety vests, portable cameras) for Statewide Compliance and Outreach Program (SCOP) teams to use while in the field.
- Received updated training related to active shooter, de-escalation, and communication techniques when encountering taxpayers who are upset. In addition, team members are reminded to avoid unsafe areas and remove themselves from situations that they determine to be dangerous.
- Conducted site safety assessments and has implemented several safety measures at the field offices to prevent burglary, theft, and counterfeit currency.
- Adhered to policies surrounding physical and facility security (i.e., alarm testing, badge access, visitor badging, etc.).

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