

December 27, 2023

Joe Stephenshaw, Director
California Department of Finance
915 L Street
Sacramento, CA 95814

Dear Director Joe Stephenshaw,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the California Privacy Protection Agency 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 Tiffany Garcia, Chief Deputy Executive Director, at (916) 905-5451, tiffany.garcia@coppa.ca.gov.

GOVERNANCE

Mission and Strategic Plan

In November 2020, voters approved Proposition 24, The California Privacy Rights Act of 2020 (CPRA). The CPRA cements California's place as the nation's leader in consumer privacy by amending and extending the California Consumer Privacy Act of 2018 (CCPA), the first comprehensive consumer privacy law in the United States. The law protects consumers' rights, including the constitutional right of privacy. To this end, it gives consumers various rights to limit and control businesses' collection and sharing of personal information and imposes various disclosure, security, and other responsibilities on businesses.

The mission of the California Privacy Protection Agency (CPPA) is to protect Californians' consumer privacy. The CPPA implements and enforces the CCPA. Its responsibilities include:

- 1) rulemaking in a highly complicated, technical, sometimes contested, and nuanced area;
- 2) supporting awareness across California's diverse population on issues related to privacy and data security, including the new rights provided to them by the law; and
- 3) preparing for meaningful administrative enforcement of those rights.

Control Environment

Under the direction of the Executive Director and the Chief Deputy Executive Director, the executive team maintains high ethical standards and attentive oversight of the Agency. The Agency is governed by a five-member board, which provides oversight of the executive team. The Board delegates all aspects of the operations of the Agency to the Executive Director, except for regulations and resolution of enforcement. CPPA maintains a managerial hierarchy to ensure that policies and procedures are developed and effectively communicated throughout the Agency. CPPA's organizational structure provides for the

delegation of decision-making authority to the most qualified staff at various management levels. This structure groups employees by division and function to ensure the appropriate segregation of duties and sufficient levels of review of staff work. This structure also allows for the effective execution of duties and ensures accountability within the chain of command.

The CPPA prioritizes extensive job outreach to diverse, qualified candidates and comprehensive staff development to establish and maintain a competent workforce. The Department of General Services (DGS), Office of Human Resources supports the Agency in this work through contracted services. CPPA works with DGS and the CPPA Public Affairs team to advertise job postings and conduct extensive outreach to prospective candidates through popular job-search platforms and social media. For positions requiring specific qualifications, such as a law degree, CPPA staff shares job postings with diverse legal associations and their listservs. CPPA seeks to ensure that the pool of candidates is representative of the state's diversity.

The CPPA also prioritizes staff development to help maintain an efficient workforce. The Agency provides training opportunities for employees. Management provides timely feedback to employees during the probationary period to ensure skills are aligned with the Agency's objectives. Management and senior staff provide ongoing coaching and mentorship to facilitate professional growth. Executive staff receive annual reviews to help motivate and hone their skills to support the Agency's mission.

CPPA has three levels of accountability. First, board members serve at the pleasure of their appointing authority and can be removed at any time. Second, board members conduct an annual evaluation of the Executive Director (ED), who is responsible for the Agency's operations. Board members provide information to the board chair on the ED's performance, and the board chair shares the findings with the ED in a closed-session meeting. The ED is an at-will employee who serves at the pleasure of the board. Third, CPPA employees are civil service employees, and their conditions of employment are governed by civil service laws and regulations and by collective bargaining agreements. Management provides feedback and assessment during probationary reports and annual reviews to ensure that employees are meeting the requirements of their roles as indicated in their duty statements. If an employee is not meeting the expectations of their position, managers provide guidance and resources.

Information and Communication

Information for Operational, Programmatic, and Financial Decision-Making

Management oversees the use of information critical to department operations. Programmatic and operational information is discussed on a weekly basis by the executive team. Under the oversight of the Chief Deputy Executive Director, the Administration Division, in collaboration with CPPA program areas are responsible for providing financial decision-making information. Monthly financial reports are developed internally and provided to each Deputy Director, and the Deputy Directors meet with the CPPA Budget Manager to discuss budgetary changes.

Channels for Communication

Management communicates information about policies, programs, and operations through established channels. The communication channels follow the chain of command to ensure employees throughout the Agency receive information.

In addition to the chain of command communication, the Agency uses various methods to communicate important and relevant information. Such methods include regular management and team meetings, all staff meetings, email blasts, and the CPPA Intranet. Further, the Agency has posted the state's Whistleblower Hotline on the Intranet for employees to report ethical issues. If the communication line is compromised, CPPA employees are empowered to go around the traditional chain of command.

- All external stakeholders may sign up for the Agency's listserv, which is used to update interested parties on upcoming public meetings and other pertinent news.
- Stakeholders can contact staff through info@coppa.ca.gov, which is posted on the Agency's website or the Agency's main phone number.
- Staff utilizes social media and participates in sector-specific conferences and workshops to inform practitioners in the privacy space regulated by the
- The Agency's website includes forms to file a complaint and frequently asked questions to better serve the public.
- The Agency's website is fully accessible and designed, developed, and maintained in compliance with California Government Code Sections 7405 and 11135.
- The Agency's board meetings are typically conducted in a hybrid format, giving the public the opportunity to appear in person or remotely through Zoom.
- Finally, at board meetings, per the Bagley-Keene Act, the public is provided an opportunity to comment on each agenda item in open session.

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 Privacy Protection Agency monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to: Tiffany Garcia, Chief Deputy Executive Director.

The CPPA has established an entity-wide, continuous process to ensure internal control systems are working as intended. The executive monitoring sponsor facilitates the California Privacy Protection Agency monitoring practices and verifies that they are implemented and functioning properly. The responsibilities as the executive monitoring sponsor(s) have been given to the Chief Deputy Executive Director.

The Agency's Strategic Plan is being updated, and once approved by the Board, the Agency will use Key Performance Indicators to ensure enhanced systems are monitored and stay on track.

RISK ASSESSMENT PROCESS

The following personnel were involved in the California Privacy Protection Agency risk assessment process: executive management, middle management, and front line management.

The following methods were used to identify risks: brainstorming meetings, ongoing monitoring activities, other/prior risk assessments, consideration of potential fraud, and other.

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

RISKS AND CONTROLS

Risk: Workforce Recruitment & Retention

The Agency is tasked with regulating the emerging area of consumer privacy, in which a limited number of subject matter experts exist. Further, the recruitment process through contracted services is often delayed, which presents a challenge in recruiting staff, particularly attorneys with knowledge of privacy law. A shortage of privacy attorneys results in burnout and potentially high turnover.

In addition to attorney shortage, the Agency requires technologists with privacy and cyber security expertise to conduct audits and support enforcement. The Agency is the first regulator of consumer privacy rights, including artificial intelligence, in the country. Because this is a new policy area, there is no existing state service classification for the type of expertise the Agency requires to examine privacy compliance among the regulated community. Without the existing classification, we will be forced to use other IT-related classifications, which may not meet all the necessary job requirements for privacy-focused technologists, and employees may have to perform duties outside the CalHR-approved workload for the IT classification, which could result in grievances.

Control: Temporary Staff

The Agency administratively established Graduate Legal Assistant (GLA) positions to help mitigate the Agency's workload needs and serve as a pathway to hire attorneys with the necessary expertise. In addition to GLAs, the Agency has relied on Retired Annuitants and interns to help bridge the human resource gap in the interim.

Control: Propose New Classification

Work with CalHR and other state departments with a similar need to establish the appropriate technologist classification.

Control: Recruitment

The Agency's Public Affairs Division conducts extensive outreach through various networks to find talent and share information about the Agency's work. Public Affairs

widely advertises the positions, through social media and assists in setting up speaking engagements for the Executive Team, where staff highlights the available positions. This will help attract mission-driven talent to the Agency.

Control: Organizational Structure Evaluation & Retention

As the Agency grows, the executive team will evaluate the organizational structure to ensure it aligns resources with the workload, adopt realistic internal due dates, and reduce processes or work that does not provide value. The Agency has also adopted a hybrid telework policy to allow for better work/life balance. The Agency promotes training opportunities and is working towards leadership training for the new executive team.

Control: Resources

The CPPA Board's long-term plan has been to transition administrative functions in-house. The Agency is now working on a plan to bring administrative services in-house, starting with Human Resources. This will help speed up the recruitment process and help avoid losing potential candidates due to the delayed hiring process.

Risk: External Support Dependency

The Agency contracts with other state agencies for administrative functions, including Human Resources, Fiscal Services, and Information Technology. While this was necessary when the Agency was first created, the external dependency sometimes results in operational delays, such as long lead times to fill vacancies and procurement delays, affecting the Agency's operations.

Control: Internal Capacity

CPPA plans to transition administrative functions in-house. The Agency is in the process of hiring a retired annuitant to evaluate the workload in the various areas and develop a plan for the transition.

Risk: Capacity Building

The Agency is new and has doubled in size in a year, necessitating updated processes and communication channels. As the Agency builds capacity, it must also establish appropriate processes to ensure that all staff consistently follow the same procedures and protocols. A lack of documented processes and procedures impacts productivity and could cause inconsistency in public communications.

Control: Policies and Procedures

The Agency is in the process of updating existing policies and procedures, as well as developing new ones to address emerging needs. This will help mature the organization, increase efficiency, and establish protocols, thereby improving the governance structure.

Risk: Technology Implementation

Technology implementation is a risk due to the limited expertise and funding available in the state. The Agency is currently reliant on contracted Information Technology (IT) services through the Department of Consumer Affairs, but the Agency plans to move IT in-house and build out the necessary expertise and oversight commensurate with an Agency our size and scope, governing businesses' data use and privacy/security protocols.

Control: Work Closely with Control Agencies

CPPA will work closely with control agencies including the Department of Finance and the California Department of Technology, to identify and procure the necessary resources.

CONCLUSION

The California Privacy Protection Agency 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.

Ashkan Soltani, Executive 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