CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov

Date: April 25, 2025

To: California Privacy Protection Agency Board
(Meeting of May 1, 2025)

From: Maureen Mahoney, Deputy Director of Policy and Legislation

Subject: **Agenda Item 3 — Legislative Update and Authorization of CPPA Positions on Pending Legislation. SB 468 (Becker), High risk AI systems: Duty to protect personal information, as introduced**

SB 468, authored by Senator Becker, requires deployers of high-risk AI systems that process personal information to maintain a comprehensive information security program. The bill has been approved by the California Senate Judiciary Committee and is now under consideration by the Senate Appropriations Committee. Because the bill would help better secure the troves of personal information maintained and processed by high-risk AI systems, and it gives the Agency rulemaking authority, staff recommends a "support if amended" position — specifically, support if amended to grant the California Privacy Protection Agency enforcement authority.

Summary

The California Consumer Privacy Act (CCPA) grants consumers rights with respect to personal information that is collected, used or sold by a business. The CCPA requires businesses to implement "reasonable security procedures and practices." The law also instructs the California Privacy Protection Agency (CPPA or Agency) to issue regulations requiring businesses whose processing of personal information presents a significant risk to privacy or security to perform annual cybersecurity audits. The Agency has initiated formal rulemaking for proposed regulations establishing the requirements for cybersecurity audits.

This bill creates a new section in the Civil Code that imposes a duty on covered deployers to protect personal information held by the deployer with a comprehensive information security program that meets specifications set forth in the bill. Covered deployers are defined as businesses that deploy high-risk AI systems that process personal information.

The bill requires covered deployers to have written information security programs that designate employee managers, provide for regular assessment of reasonably foreseeable internal and external risks, include restrictions on physical access to records, and establish regular monitoring and review to determine that safeguards are working properly. The program must also have detailed employee protocols including ongoing education and training, methods for detecting non-compliance,

and disciplinary measures for violations. The bill also requires incident response requirements, secure user authentication protocols, secure access control measures, and encryption for specified data transmission.

The bill provides that the California Privacy Protection Agency may adopt implementing regulations pursuant to the Administrative Procedure Act (APA). It specifies that any regulation to establish fees shall be exempt from the APA.

Violations of the bill constitute a deceptive trade act or practice under the Unfair Competition Law.

Analysis

In staff's view, this bill is consistent with the Agency's mission to protect Californians' consumer privacy. AI systems present unique security vulnerabilities stemming from their complexity, massive scale, and handling of vast quantities of personal information across large networks. High-risk AI systems, by definition, collect and process enormous volumes of sensitive data needed to make legally significant decisions about housing, education, employment, health care or criminal justice. As large repositories of sensitive personal information, these systems are prime targets for breaches, misuse, and unauthorized access that could lead to identity theft, discrimination, harassment, or financial harm. Clear, sufficient mandated information security protocols would help protect consumers' critical personal information.

Additionally, the rulemaking authority granted to the CPPA under the bill allows the Agency to provide additional clarity as needed and make sure that these security requirements align with the obligations of the CCPA and our cybersecurity regulations. However, the Agency should also be granted enforcement authority. As the entity developing regulations, it can efficiently determine whether businesses are meeting their obligations under the law and regulations. We recommend that the bill be amended to grant the CPPA enforcement authority.

Recommendation: Support if amended to grant the CPPA enforcement authority

Public Support/Opposition

Per the April 18, 2025 Senate Judiciary Commitee bill analysis[1]:

<u>Support</u>

Oakland Privacy
Transparency Coalition.AI

<u>Opposition</u>

California Hospital Association

[1] California Senate Judciary Committee bill analysis at 12 (April 18, 2025), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202520260SB468.

Staff Contact: Maureen Mahoney, Deputy Director of Policy & Legislation
maureen.mahoney@cppa.ca.gov