CALIFORNIA PRIVACY PROTECTION AGENCY

TITLE 11. LAW
DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY
CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

NOTICE OF PROPOSED RULEMAKING

Notice published November 22, 2024

Subject Matter of Proposed Regulations: Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies. (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)

Sections Affected: California Code of Regulations (CCR), Title 11, sections 7001, 7002, 7003, 7004, 7010, 7011, 7012, 7013, 7014, 7015, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7027, 7028, 7050, 7051, 7053, 7060, 7062, 7063, 7070, 7080, 7102, 7120, 7121, 7123, 7124, 7150, 7151, 7152, 7153, 7154, 7155, 7156, 7157, 7200, 7201, 7220, 7221, 7222, 7270, 7271, 7300, and 7302.

The California Privacy Protection Agency (Agency) proposes to amend and adopt the proposed regulations, described below, after considering all comments, objections, and recommendations regarding the proposed action.

PUBLIC HEARING

The Agency will hold a public hearing to provide all interested persons an opportunity to present oral or written statements or arguments with respect to the proposed regulations:

Date:	Tuesday, January 14, 2025
Time:	2:00–6:00 p.m. Pacific Time
Location:	Cannabis Control Appeals Panel Hearing Room 400 R Street, Suite 330 Sacramento, CA 95811

To join this hearing by virtually by online video platform:
https://cppa-ca-gov.zoom.us/j/81402254127

Or Telephone:
USA (216) 706-7005 US Toll
USA (866) 434-5269 US Toll-free
Conference code: 682962

Please contact Candice Sanders at regulations@cppa.ca.gov or (916) 642-7558 by 4:30 p.m. on Friday, January 10, 2025, if reasonable accommodations are necessary.

At the hearing, any person may present oral or written statements or arguments relevant to the proposed action described in the Informative Digest. Participants will be given instructions on how to provide oral comment once they have accessed the hearing. The Agency requests, but does not require, that persons who make oral comments at the hearing also submit a written copy of their testimony at, or immediately following, the hearing via email to regulations@cppa.ca.gov.

WRITTEN COMMENT PERIOD

Any interested person, or their authorized representative, may submit written comments relevant to the proposed regulatory action. The written comment period closes on January 14, 2025, at 6:00 p.m. Pacific Time. Only written comments received by that time will be considered. Within your comment, please indicate the proposed rulemaking action to which your comment refers to at the top of the page: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Please submit written comments to:

EMAIL: regulations@cppa.ca.gov

Please include "Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations" in the subject line.

MAIL: California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

Written and oral comments, attachments, and associated contact information (e.g., address, phone, email, etc.) become part of the public record and will be posted on our public website: https://cppa.ca.gov/regulations/ccpa_updates.html

AUTHORITY AND REFERENCE

Authority: Section 1798.185, Civil Code.

Reference: Sections 1798.81.5, 1798.100, 1798.105, 1798.106, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.35, 1798.199.40, 1798.199.45, 1798.199.50, and 1798.199.65, Civil Code.

INFORMATIVE DIGEST/POLICY STATEMENT OVERVIEW

Summary of Existing Laws and Regulations:

The California Consumer Privacy Act (CCPA) was enacted in 2018 and became effective in 2020. It granted consumers new privacy rights and imposed obligations on businesses that collect personal information about consumers. The CCPA provided consumers with the rights to know about personal information collected by businesses, delete personal information, opt out of the sale of personal information, and be protected from discrimination in service and price when exercising privacy rights. In 2020, the Consumer Privacy Rights Act (CPRA) amended the CCPA, creating the Agency and granting consumers additional rights, such as the rights to correct, limit the use and disclosure of sensitive personal information, and opt-out of the sharing of their personal information. In addition, the CPRA created or amended certain requirements for businesses, such as those relating to the processing of consumers' personal information, disclosures to consumers, and methods for submitting CCPA requests.

Although the Attorney General initially had rulemaking authority to implement the CCPA, that authority transferred to the Agency in 2022. Subsequently, the Agency engaged in rulemaking to amend the regulations previously adopted by the Attorney General, operationalize the CPRA amendments to the CCPA, and provide additional clarity and specificity to implement the law. In March 2023, the Agency's first formal rulemaking process concluded, and its regulations became effective.

In September 2024, the Governor signed into law three bills that amend the CCPA and become effective January 1, 2025. AB 1008 (2023-2024) amends the definition of personal information to clarify that it includes physical, digital, and abstract digital formats, including metadata or artificial intelligence ("AI") systems capable of outputting personal information. SB 1223 (2023-2024) expands the definition of sensitive personal information to include "neural data." Therefore, when the CCPA and existing and proposed regulations reference personal information or sensitive personal information, those references are intended to encompass the definitions of those terms contained in these bills as the proposed regulations would be adopted after January 1, 2025.

AB 1824 requires businesses to which personal information is transferred as an asset during certain transactions, such as a merger or acquisition, to honor consumers' opt-out of sale/sharing preferences. The CCPA's requirements for the right to opt-out of sale/sharing,

including in the existing or proposed regulations, also apply to businesses to which personal information is transferred.

Effect of the Proposed Rulemaking:

The proposed regulations include updates to existing Agency regulations, as well as the addition of regulations related to cybersecurity audits, risk assessments, automated decisionmaking technology (ADMT), and insurance requirements. The updates to existing regulations modify the regulations to be consistent with current law, refine the existing regulations based on the Agency's experience and available information since the time these regulations were adopted, and make changes without regulatory effect. The Agency has identified that there is a need to provide clarity to the regulated industry about the interplay between insurance laws and the CCPA; thus, the Agency has included regulations related to insurance requirements. Finally, the Agency is statutorily mandated to adopt regulations to implement and clarify requirements related to cybersecurity audits, risk assessments, and ADMT. The proposed regulations seek to fulfill that mandate.

Article 1. General Provisions.

Article 1 of the Agency's regulations contain general provisions including definitions, restrictions on collection and use of personal information, disclosures and communications with consumers, and requirements for methods of submitting CCPA requests and obtaining consumer consent. The proposed regulations would amend section 7001 to define the following terms: "artificial intelligence," "automated decisionmaking technology" and "ADMT," "behavioral advertising," "cybersecurity audit," "cybersecurity program," "deepfake," "information system," "multi-factor authentication," "penetration testing," "performance at work," "performance in an educational program," "physical or biological identification or profiling," "privileged account," "profiling," "publicly accessible place," "request to access ADMT," "request to appeal ADMT," "request to opt-out of ADMT," "right to access ADMT," "right to opt-out of ADMT," "systematic observation," "train automated decisionmaking technology or artificial intelligence," and "zero trust architecture." The proposed regulations would also amend the definitions of "nonbusiness," "request to know," "sensitive personal information," and "verify."

The proposed regulations would amend section 7002 to clarify that a business must allow a consumer to withdraw consent to collecting and processing personal information, unless an exception applies, and require that businesses comply with all of the requirements within that section for additional collection or processing of personal information.

The proposed regulations would also amend the requirements of section 7003 regarding the appearance of privacy related links on a business website. The proposed regulations would further require mobile applications to include a conspicuous link within the application itself.

Additionally, the proposed regulations would amend section 7004 to clarify that businesses must incorporate the principles listed in the section in designing and implementing their methods for submitting CCPA requests and for obtaining consumer consent. The proposed regulations would revise and add to the examples provided in the section, replace permissive language with mandatory language for requirements, and address how requests for consent must appear. The proposed regulations would prohibit businesses from using misleading statements or omissions, affirmative misstatements, or deceptive language in obtaining consent, as well as categorize choices that are driven by a false sense of urgency as misleading. The proposed regulations would establish that a consumer's silence or failure to act affirmatively does not constitute consent. The proposed regulations would further clarify that methods must be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. The proposed regulations further clarify that this principle also applies to methods for providing and withdrawing consent and reminds businesses that individuals handling phone calls from consumers submitting CCPA requests must have the knowledge and ability to process those requests. The proposed regulations clarify the illustrative examples in subsection (a) were a non-exhaustive list and that a user interface that has the effect of subverting or impairing consumer choice is a dark pattern.

Article 2. Required Disclosures to Consumers.

Article 2 contains required disclosures to consumers. The proposed regulations would amend section 7010 to require a business that uses ADMT to provide consumers with a Pre-use Notice, which must include a link through which consumers can opt-out of the business's use of ADMT. The proposed regulations clarify exceptions to the requirement to provide an opt-out link to consumers.

The proposed regulations would amend section 7011 to require mobile applications to include a link to the privacy policy. Businesses would also be required to describe categories of sources and categories of third parties in a manner that provides consumers a meaningful understanding of those things. The proposed regulations would clarify that disclosures for a business purpose are to service providers and contractors, not third parties. The proposed regulations also clarify that businesses must include an explanation of consumers' right to opt-out of ADMT and an explanation of the right to access ADMT, if it is using ADMT. The proposed regulations clarify that consumers have a right against retaliation when exercising their privacy rights, and that this right also applies when they are acting as an applicant to an educational program, a job applicant, or a student. The proposed regulations would also require the business to provide a general description of the process it uses to verify a consumer's "request to access ADMT."

The proposed regulations would amend section 7013 to provide more examples of the requirement that the Notice of Right to Opt-Out of Sale/Sharing be provided in the same manner in which the business collects the personal information that it sells or shares.

The proposed regulations would amend section 7014 to further implement Civil Code section 1798.135, subdivision (a)(2), by requiring the notice of the consumer's right to limit the use of sensitive personal information be provided in the same manner in which the business collects the sensitive personal information, and provides examples. The proposed regulations would also amend section 7015 to allow for the adjustment of color to ensure that the opt-out icon is conspicuous and easy to read.

Article 3. Business Practices for Handling Consumer Requests.

Article 3 contains requirements for how consumer requests must be handled by businesses. The proposed regulations would amend section 7020 to require businesses to provide a means by which the consumer can request that the business, in response to a request to know, provide personal information collected prior to the 12-month period preceding the business's receipt of the request. The proposed regulations would also amend section 7021 to make requests to access ADMT and to appeal ADMT subject to the timelines contained in the section.

Additionally, the proposed regulations would amend section 7022 by clarifying what a business must do in response to a request to delete. This includes that businesses, service providers, and contractors are to implement measures to ensure that information subject to a request to delete remains deleted, deidentified, or aggregated. The proposed regulations would also explain that whether a business, service provider, or contractor has implemented these measures factors into whether they have complied with the consumer's request to delete, and that they should consider and address how previously deleted information may be recollected. The proposed regulations would also require a business that denies a request to delete in whole or in part to inform the consumer that they can file a complaint with the Agency and the Attorney General's office.

The proposed regulations would also amend section 7023 to clarify that businesses, service providers, and contractors are to implement measures to ensure that information subject to a request to correct remains corrected and that a business is obligated to correct information stored in a backup or archived system only if that system comes into active use. The proposed regulations would require businesses that deny a consumer's request to correct to inform the consumer that, upon the consumer's request, it will note both internally and to any person to whom it discloses the personal information that the accuracy of the personal information is contested by the consumer. The proposed regulations would require a business to make a written statement the consumer submits available to any person to whom it discloses the personal information subject to the request to correct health information. Additionally, businesses would be required to provide the name of the source from which it received alleged inaccurate information, or inform the source that the information provided was incorrect and must be corrected. The proposed regulations require businesses to confirm certain information they maintain is the same as what the consumer has provided and clarifies that failing to address the possibility that corrected information may be overridden by inaccurate information

factors into whether the business, service provider, or contractor has adequately complied with a consumer's request to correct. The proposed regulations also clarify that complaints may be filed with the Agency or Attorney General's office.

The proposed regulations would amend section 7024 to require businesses to provide a way for consumers to confirm that certain sensitive personal information the business maintains is what the consumer believes it should be and that when a business denies a request to know in whole or in part, it must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. The proposed regulations would more precisely explain a business's disclosure obligations under Civil Code sections 1798.110 and 1798.115 and clarify that businesses must identify categories of service providers and contractors in a manner that provides consumers a meaningful understanding of the categories listed.

The proposed regulations would amend section 7025 to require businesses to display the consumer's choice as it relates to the sale/sharing of their personal information; the business must display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. Exemplar language for how a business can communicate this information to the consumer is included in the proposed regulations.

The proposed regulations would amend section 7026 to require that a business that denies a request to opt-out of sale/sharing to inform the consumer that they can file a complaint with the Agency and the Attorney General's office. Illustrative examples to explain the timing requirements for requests to opt-out of sale/sharing have been included. The proposed regulations would require businesses to provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed and provide exemplar language for how a business can communicate this information to the consumer.

The proposed regulations would amend section 7027 to include the requirement that when a business denies a request to limit, it must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. "Shared" has been replaced with "made available" to be more precise and additional examples have been included. The proposed regulations would also require businesses to provide a means by which the consumer can confirm that their request to limit has been processed.

The proposed regulations would amend section 7028 to extend the procedures for requests to opt-in to include requests to opt-in to the sharing of personal information and requests to opt-in to the use and disclosure of sensitive personal information. The proposed regulations address situations where consumers initiate transactions with businesses after making a request to limit when those transactions may require that the business disclose or use the consumer's sensitive personal information in a manner inconsistent with the request to limit, allowing a business to obtain the consumer's consent to use or disclose the information for that purpose even if it is within 12 months of the consumer's request. The proposed regulations would also clarify that section 7004 applies to obtaining the consumer's consent.

Article 4. Service Providers, Contractors, and Third Parties.

Article 4 of the proposed regulations contains the requirements related to service providers, contractors, and third parties. The proposed regulations would amend section 7050 to clarify that the purposes for which a service provider or contractor retains, uses, or discloses personal information must be reasonably necessary and proportionate to serve the purposes listed in the regulation and provides an example. The proposed regulations would also require that service providers and contractors cooperate with businesses for those businesses' cybersecurity audits and risk assessments with respect to the personal information that the service provider or contractor has collected pursuant to their written contract with the business. The proposed regulations would explain that cooperating with a business's completion of its cybersecurity audit includes making available to the business's auditor all relevant information that the auditor requests and not misrepresenting any fact that the auditor deems relevant to the audit. The proposed regulations would also explain that cooperating with a business that is conducting a risk assessment includes making available to the business all facts necessary to conduct the risk assessment and not misrepresenting any fact necessary to conduct the risk assessment.

The proposed regulations would amend section 7051 by including additional examples of requirements that a business may include in its contracts with service providers or contractors.

Article 5. Verification of Requests.

Article 5 contains the responsibilities of businesses to verify that the person making the request is also the subject of the information impacted by the request. The proposed regulations would amend section 7060 to include requests to access and to opt-out of ADMT. The proposed regulations would clarify that businesses must first consider how they can verify a consumer's identity using personal information that they already maintain about the consumer before asking the consumer to provide additional information. The proposed regulations would make certain requirements mandatory when verifying requests and require a business that compensates the consumer for the cost of the notarization to provide the consumer with instructions on how they will be reimbursed prior to the consumer's submission of the notarization. The proposed regulations would also extend the requirement to implement "reasonable security measures" to information about a business's use of ADMT with respect to a consumer. The proposed regulations would clarify that a business must not use personal information that is the subject of a request to correct to verify the consumer.

The proposed regulations would amend section 7062 to include "request to access ADMT."

The proposed regulations would also amend section 7063 to clarify that businesses shall not require consumers to resubmit their request in their individual capacity.

Article 6. Special Rules Regarding Consumers Less Than 16 Years of Age.

The proposed regulations would modify the title of the article to use the term "less than" instead of "under" to be consistent with the content within the article.

Article 7. Non-Discrimination.

The proposed regulations would amend section 7080 to include requests to access and to opt-out of ADMT.

Article 8. Training and Record-Keeping.

The proposed regulations would amend section 7102 to require the compilation and disclosure of metrics for requests to access and to opt-out of ADMT that the business received, complied with in whole or in part, and denied.

Article 9. Cybersecurity Audits.

Article 9 of the proposed regulations would be a new article containing the requirements for cybersecurity audits. The proposed regulations would add section 7120 that explains which businesses' processing presents significant risk to consumers' security. The proposed regulations would clarify that a business that "meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year" is a business whose processing of consumers' personal information presents significant risk to consumers' security. The proposed regulations would identify a business that meets the annual gross revenue threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A), and one of two processing thresholds in the preceding calendar year as presenting significant risk to consumers' security. The proposed regulations would clarify that the two processing thresholds are met if the business processed either (1) the personal information of 250,000 or more consumers or households, or (2) the sensitive personal information of 50,000 or more consumers.

The proposed regulations would add section 7121, which provides a business with 24 months from the effective date of the proposed regulations to complete its first cybersecurity audit and subsequently requires one every calendar year, with no gap in the months covered by successive cybersecurity audits.

The proposed regulations would add section 7122, which contains the requirements for thorough and independent cybersecurity audits. The proposed regulations would require use of a qualified, objective, independent auditor who uses procedures and standards generally accepted in the profession of auditing; and provide guidance as to what auditor objectivity and independence mean, and how businesses must preserve auditor independence. For example, the proposed regulations would clarify that the auditor must exercise impartial judgment, be

free to make decisions and assessments without influence by the business, and not participate in the very business activities that the auditor may assess in the current or subsequent cybersecurity audits. If the auditor is internal, the proposed regulations would require that they report directly to, and have their performance-evaluation and compensation determined by, the business's board, governing body, or the business's highest-ranking executive who does not have direct responsibility for the cybersecurity program. The proposed regulations would require a business to make all information available to the auditor that the auditor requests as relevant, make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit, and not misrepresent any fact relevant to the cybersecurity audit. The proposed regulations would specify that the audit must articulate its scope and criteria; identify the specific evidence examined to make decisions and assessments; explain why the scope, criteria, and evidence are appropriate; explain why the specific evidence examined is sufficient to justify the auditor's findings; not rely primarily on assertions or attestations but rather on specific evidence that the auditor deemed appropriate; assess, document, and summarize each applicable component of the business's cybersecurity program; identify gaps or weaknesses in the business's cybersecurity program; and address the status of any gaps or weaknesses identified in any prior cybersecurity audit, and any corrections or amendments to any prior cybersecurity audit. The proposed regulations would also require the audit to include the auditor's name, affiliation, and relevant qualifications; as well a signed statement by each auditor certifying that they completed an independent review, exercised objective and impartial judgment, and did not rely primarily on assertions or attestations by the business's management. The proposed regulations would require the audit to be reported to the business's board, governing body, or highest-ranking executive responsible for its cybersecurity program and to contain a signed statement by that person certifying that the business did not influence, and made no attempt to influence, the auditor's decisions or assessments, as well as that they have reviewed, and understand the findings of, the cybersecurity audit. The auditor would be required to retain all documents relevant to each cybersecurity audit for a minimum of five (5) years.

The proposed regulations would add section 7123, which contains what the cybersecurity audit must cover. The proposed regulations would require the audit to identify, assess, and document how the business's cybersecurity program (that is appropriate to the business's size, complexity, and the nature and scope of its processing activities) protects personal information from unauthorized actions; and identify, assess, and document 18 components of the business's cybersecurity program, as applicable, or explain why a component is not necessary and how the safeguards the business has in place provide at least equivalent security.

The components include: (1) authentication, including multi-factor authentication and strong unique passwords or passphrases; (2) encryption of personal information, at rest and in transit; (3) zero trust architecture; (4) account management and access controls, including restricting access to personal information and functions to what is necessary for that person to perform their duties; the number of privileged accounts and their functions, using a privileged-access

management solution; the creation of new accounts and ensuring that their access and privileges are limited; and restricting and monitoring physical access to personal information; (5) inventory and management of personal information and the business's information system, including inventories, classification, and tagging of personal information; hardware and software inventories and the use of allowlisting; hardware and software approval processes and preventing the connection of unauthorized hardware and devices to the business's information system; (6) secure configuration of hardware and software, including software updates and upgrades; securing on-premises and cloud-based environments; masking sensitive and other personal information as appropriate by default in applications; security patch management; and change management; (7) internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting; (8) audit-log management, including the centralized storage, retention, and monitoring of logs; (9) network monitoring and defenses, including the deployment of bot-detection and intrusion-detection and intrusion-prevention systems, and data-loss-prevention systems; (10) antivirus and antimalware protections; (11) segmentation of an information system; (12) limitation and control of ports, services, and protocols; (13) cybersecurity awareness, education, and training, including training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system; and how the business maintains current knowledge of changing cybersecurity threats and countermeasures; (14) secure development and coding best practices, including code-reviews and testing; (15) oversight of service providers, contractors, and third parties; (16) retention schedules and proper disposal of personal information no longer required to be retained by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information to make it unreadable or undecipherable through any means; (17) how the business manages its responses to security incidents; and (18) the business's business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.

The proposed regulations also would require the audit to describe how the business implements and enforces compliance with the applicable components, how effective the business's cybersecurity program components are at protecting consumers' personal information, the status of any gaps or weaknesses of the applicable components, and the business's plan to address them. The proposed regulations would require the audit to include the titles of individuals responsible for the business's cybersecurity program; and the date that the program and any evaluations of it were presented to the business's board, governing body, or to the business's highest-ranking executive responsible for the program. The audit would also be required to include a sample copy or a description of any required notification to a consumer or any agency with jurisdiction over privacy laws or other data processing authority, as well as dates and details of the activity that gave rise to the required notifications and any related remediation measures taken by the business. The proposed regulations would also clarify that if a business has engaged in a cybersecurity audit, assessment, or evaluation that meets all of the requirements of Article 9, the business is not required to complete a duplicative cybersecurity audit, but must explain how what it has already done meets all of the regulatory

requirements, and supplement it with additional information if it does not meet all such requirements.

The proposed regulations would add section 7124, which provides for businesses required to complete a cybersecurity audit to submit to the Agency every calendar year a written certification that the business completed the cybersecurity audit. The certification would be submitted to the Agency through https://cppa.ca.gov/, identify the 12 months that the audit covers, be signed by a member of the business's board, governing body, or highest-ranking executive with authority to certify on behalf of the business and who is responsible for oversight of the business's cybersecurity-audit compliance, and include a statement certifying that the signer, identified by name and title, has reviewed and understands the findings of the cybersecurity audit.

Article 10. Risk Assessments.

Article 10 would be a new article containing the requirements for risk assessments. The proposed regulations would add section 7150 to address when a business must conduct a risk assessment, which is when their processing of consumers' personal information presents significant risk to consumers' privacy. The proposed regulations would require a risk assessment when a business sells or shares personal information; or processes sensitive personal information, except for when a business processes sensitive personal information solely and specifically for administering compensation payments, determining and storing employment authorization, administering employment benefits, or for wage reporting as required by law. A risk assessment would also be required when a business uses ADMT for a significant decision concerning a consumer or for extensive profiling. For this purpose, "significant decision" would mean a decision that results in access to, or the provision or denial of financial or lending services; housing; insurance; education enrollment or opportunity; criminal justice; employment or independent contracting opportunities or compensation; healthcare services; or essential goods or services. The proposed regulations would clarify that "education enrollment or opportunity" includes admission or acceptance into academic or vocational programs, educational credentials, and suspension and expulsion; and that "employment or independent contracting opportunities or compensation" includes hiring, allocation/assignment of work and compensation, promotion; and demotion, suspension, and termination. The proposed regulations would also explain that "significant decisions" include only decisions using information that is not subject to relevant data-level exceptions in the CCPA. The proposed regulations would define "extensive profiling" to include profiling consumers in work and educational contexts, in public, or for behavioral advertising. The proposed regulations would further identify processing of personal information to train ADMT or AI that is capable of being used for a significant decision, to establish individual identity, for physical or biological identification or profiling, for the generation of a deepfake, or for the operation of generative models, as a significant risk to consumers' privacy requiring a risk

assessment. Illustrative examples of when a business must conduct a risk assessment are also included.

The proposed regulations would add section 7151, which requires businesses to ensure that relevant individuals at the business prepare, contribute to, or review the risk assessment, based upon their involvement in the processing activity. "Relevant" individuals are those whose job duties pertain to the processing activity, and examples of these types of individuals are included. The proposed regulations would require relevant individuals to make good-faith efforts to disclose all facts necessary to conduct the risk assessment and not misrepresent any facts. The proposed regulations would clarify that a risk assessment may involve external parties to identify, assess, and mitigate privacy risks, and include examples of the types of external parties that may be involved in the risk-assessment process.

The proposed regulations would add section 7152, which contains the requirements for the risk assessment and clarifies that the purpose of a risk assessment is to determine whether the risks to consumers' privacy outweigh the benefits for a given processing activity. It also explains how a business must conduct a risk assessment. Businesses would be required to identify why they will be processing consumers' personal information and would be prohibited from identifying this purpose in generic terms. The proposed regulations would also require businesses to identify the categories of personal information to be processed, whether they include sensitive personal information, and the minimum personal information necessary to achieve the purpose of the processing. The proposed regulations would also require a business to identify its actions to maintain data quality for certain uses of ADMT or AI, and the proposed regulations would provide a definition of "quality of personal information," which includes completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of sources. Examples are included of the types of actions a business may take, such as identifying the source of the personal information and whether that source is reliable; identifying how the personal information is relevant to the task being automated and how it is expected to be useful for the development, testing, and operation of the ADMT or AI; identifying whether the personal information contains sufficient breadth to address the range of real-world inputs the ADMT or AI may encounter; and identifying how errors from data entry, machine processing, or other sources are measured and limited. The proposed regulations would also require a business to identify the operational elements of the processing activity: the planned method of processing and the sources of personal information; the length of, and criteria for, retention; the relationship between the consumer and the business; the approximate number of consumers whose personal information the business seeks to process; relevant disclosures made to the consumer, how they were made, and relevant actions to make the disclosures specific, explicit, prominent, and clear to the consumer; names or categories of relevant entities in the processing activity, the purpose for disclosing personal information to them, and actions taken to make the consumer aware of these entities' involvement; and the technology to be used, including the logic of the relevant ADMT, its output, and how the business will use that output.

The proposed regulations would require a business to specifically identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information. It provides an example of what would not meet the specificity requirement. The proposed regulations would require a business that profits monetarily from the activity to identify this benefit and, when possible, estimate the expected profit, while clarifying that benefits cannot be stated in a generalized manner. The business would also be required to specifically identify the negative impacts to consumers' privacy associated with the processing, including the sources and causes of these negative impacts and any criteria used to make these determinations. Different types of negative impacts to consumers' privacy that the business may consider are included. The proposed regulations would require a business to identify the safeguards it plans to implement to address the negative impacts, and would include different safeguards that a business may consider.

The proposed regulations would require businesses to identify, for certain uses of ADMT, whether they evaluated the ADMT to ensure it works as intended and does not discriminate based upon protected classes. The proposed regulations would also require the business to identify the policies, procedures, and training the business has implemented or plans to implement to ensure the ADMT works as intended and does not discriminate. The proposed regulations would clarify that when a business has obtained the ADMT from another person, it must identify whether it reviewed that person's evaluation of the ADMT, including any requirements or limitations relevant to the business's proposed use, as well as any accuracy and nondiscrimination safeguards the business implemented or plans to implement. Examples are included.

The proposed regulations would also require a business to identify whether it will initiate the processing activity that triggered the risk assessment. The proposed regulations would require businesses to identify who contributed to the risk assessment, when it was reviewed and approved and by whom, the individual who decides whether the business will initiate the processing activity; and if a business presents the risk assessment for review to its board of directors, governing body, or highest-ranking executive responsible for oversight of risk-assessment compliance, then the business must include the date of that review.

The proposed regulations would add section 7153, which requires businesses that make ADMT or AI available to other businesses to provide all necessary facts to those recipient-businesses to conduct their own risk assessments and provide a plain language explanation of any relevant requirements or limitations associated with the permitted uses of that technology. The proposed regulations would limit this requirement to ADMT or AI trained using personal information. The proposed regulations would add section 7154, which prohibits businesses from processing personal information for specified processing activities if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing.

The proposed regulations would add section 7155, which addresses the timing requirements for risk assessments. The proposed regulations would require businesses to conduct and document their risk assessments before initiating any of the activities triggering a risk assessment, and would require them to review their risk assessments at least once every three years for accuracy and update them as needed. The proposed regulations would also require businesses to immediately update their risk assessments whenever there is a material change to the processing activity. The proposed regulations clarify that a change is material when it diminishes the benefits of the activity, creates new negative impacts or increases their likelihood or magnitude, or diminishes the effectiveness of safeguards. The proposed regulations include examples. The proposed regulations require businesses to retain their risk assessments for as long as the activity continues, or for five years after completion of the risk assessment, whichever is later. Businesses would be required to conduct a risk assessment for any processing activity triggering a risk assessment that is ongoing after the effective date of these proposed regulations within 24 months of the effective date of these proposed regulations.

The proposed regulations would add section 7156, which explains that a business may conduct a single risk assessment for a comparable set of processing activities. It defines "comparable set of processing activities" as a set of similar processing activities that present similar risks to consumers' privacy and provides an example. Businesses that conduct and document a risk assessment to comply with another law or regulation would not be required to conduct a duplicative risk assessment. If that risk assessment does not meet all of the risk-assessment requirements of Article 10, a business must supplement the risk assessment with any required information to meet all of the requirements of these proposed regulations.

The proposed regulations would add section 7157, which establishes when a business must submit risk-assessment materials to the Agency. The proposed regulations would require businesses to submit their first risk-assessment materials to the Agency within 24 months of the effective date of these proposed regulations and subsequently, every calendar year with no gap in the months covered by successive submissions. The proposed regulations would address which risk-assessment materials must be submitted to the Agency. This includes a written certification that the business has conducted its risk assessments as set forth in Article 10, a certification from the highest-ranking executive who is responsible for oversight of the business's risk-assessment compliance, that specifies: (1) which months the business is certifying compliance for, and the number of risk assessments that were conducted and documented during that time; (2) an attestation that the designated executive has reviewed, understood, and approved the risk assessments; (3) an attestation that the business initiated any of the activities set forth in subsection 7150(b) only after conducting and documenting a risk assessment; and (4) the designated executive's name, title, signature, and date of certification. The proposed regulations would require a business to submit an abridged form of its new or updated risk assessments to the Agency in the business's annual submissions, which includes: (1) identification of which activity in triggered the risk assessment; (2) a plain language

explanation of the purpose for processing consumers' personal information; (3) the categories of personal information processed, and whether they include sensitive personal information; and (4) a plain language explanation of the safeguards that the business has implemented or plans to implement for that activity, unless providing the information would compromise security, fraud prevention, or safety. The proposed regulations would allow the business the option to include in its submission to the Agency a hyperlink to a public webpage that contains its unabridged risk assessment. The proposed regulations would not require businesses to submit a risk assessment if they do not initiate the processing activity subject to that risk assessment or to submit an updated abridged risk assessment if there is no change to a previously submitted abridged risk assessment. The proposed regulations would require businesses to submit risk-assessment materials through the Agency's website at https://cppa.ca.gov/ and to provide their unabridged risk assessments within 10 business days of a request from the Agency or the Attorney General.

Article 11. Automated Decisionmaking Technology.

Article 11 would be a new article containing the requirements for businesses' use of automated decisionmaking technology. The proposed regulations would add section 7200, which requires businesses to comply with the requirements for ADMT when they use it for: (1) a significant decision concerning a consumer; (2) extensive profiling of a consumer; or (3) training uses of ADMT. For this purpose, "significant decision" would mean a decision that results in access to, or the provision or denial of financial or lending services; housing; insurance; education enrollment or opportunity; criminal justice; employment or independent contracting opportunities or compensation; healthcare services; or essential goods or services. The proposed regulations would clarify that "education enrollment or opportunity" includes admission or acceptance into academic or vocational programs, educational credentials, and suspension and expulsion; and that "employment or independent contracting opportunities or compensation" includes hiring, allocation/assignment of work and compensation, promotion; and demotion, suspension, and termination. The proposed regulations would also explain that "significant decisions" include only decisions using information that is not subject to relevant data-level exceptions in the CCPA. The proposed regulations would define "extensive profiling" to include profiling consumers in work and educational contexts, in public, or for behavioral advertising. The proposed regulations would further identify training uses of ADMT as processing of personal information to train ADMT or AI that is capable of being used for a significant decision, to establish individual identity, for physical or biological identification or profiling, or for the generation of a deepfake.

The proposed regulations would add section 7201, which requires a business that uses physical or biological identification or profiling for a significant decision concerning a consumer, or for extensive profiling of a consumer, to conduct an evaluation of the physical or biological identification or profiling to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes. If the business obtained the

technology from another person, the business must review that person's evaluation, including any relevant requirements or limitations, but the business is not required to conduct its own evaluation of the ADMT. The proposed regulations would also require a business to implement policies, procedures, and training to ensure that the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate.

The proposed regulations would add section 7220, which clarifies that a business using ADMT must provide a Pre-use Notice to consumers that informs consumers about the business's use of ADMT and the consumers' rights to opt-out of, and to access information about, the business's use of ADMT. The proposed regulations would also require that the Pre-use Notice be easy-to-read and understandable to consumers, available in readable formats and necessary languages, reasonably accessible to consumers with disabilities, presented prominently and conspicuously before using ADMT, and presented in the manner in which the business primarily interacts with the consumer. The Pre-Use Notice must include: in plain non-generic language, the business's purpose for using the ADMT; the specific uses for which the ADMT is capable of being used and the categories of personal information that the business plans to process for training uses; a description of consumer's the right to opt-out of ADMT and how to submit their opt-out request, subject to any relevant exception to providing the opt-out right; if the business is relying upon the human appeal exception, how consumers may submit their appeal; a description of the consumer's right to access ADMT and how to submit their access request; that the business cannot retaliate against consumers for exercising their CCPA rights; and a plain language explanation of how the ADMT works, including (1) the logic of the ADMT and key parameters that affect its output and (2) the intended output of the ADMT and how the business plans to use it, as well as the role of any human involvement. It also provides illustrative examples. The proposed regulations would clarify that a business relying upon the security, fraud prevention, and safety exception is not required to include information that would compromise the business's ability to protect itself and consumers from: (1) security incidents that compromise personal information; (2) malicious, deceptive, fraudulent, or illegal actions; and (3) threats to consumers' physical safety. The proposed regulations would also clarify that certain components of the Pre-use Notice requirements do not apply to a business's use of ADMT solely for training uses. The proposed regulations further clarify that a business may consolidate its Pre-use Notices in different ways, provided that the consolidated notices include the information required by Article 11 for each of the business's proposed uses.

The proposed regulations would add section 7221, which explains that a business must provide consumers with the ability to opt-out of the business's use of ADMT if the ADMT is used for a significant decision, extensive profiling, or training uses of ADMT. The proposed regulations would identify exceptions to the consumer's right to opt-out of ADMT, including when it is used solely for security, fraud prevention, and safety; or in situations where consumers are provided with the ability to appeal a significant decision to a qualified human reviewer who has the authority to overturn that decision. To qualify for the latter exception, the proposed regulations would require that a human reviewer consider relevant information provided by a consumer;

and that the business provide a method of appeal that is easy to execute, require minimal steps, and comply with section 7004; and that the business respond to requests to appeal within specified timelines. The proposed regulations would also provide that a business does not need to provide an opt-out of ADMT when it uses ADMT for admission, acceptance, or hiring decisions; for allocation or assignment of work and compensation decisions; or for work or educational profiling, provided that the business's use of the ADMT is necessary for these respective purposes, that the business has evaluated its use of ADMT to ensure it works as intended for the business's proposed use and does not discriminate, and that the business has implemented accuracy and nondiscrimination safeguards. The proposed regulations would also clarify that these exceptions do not apply to profiling for behavioral advertising or to training uses of ADMT.

The proposed regulations require that businesses provide two or more methods for submitting opt-out of ADMT requests, with at least one method reflecting the manner in which the business primarily interacts with the consumer. The proposed regulations also require businesses to provide an opt-out link titled "Opt-out of Automated Decisionmaking Technology" in the Pre-use Notice if the business interacts with consumers online. Illustrative examples are provided of other acceptable opt-out methods. The proposed regulations clarify that a cookie banner or similar notification about cookies does not necessarily comply with the requirements for website methods of submission; to comply, it must notify the consumer about the right to opt-out of ADMT in specific terms. The proposed regulations would clarify that methods for submitting requests to opt-out of ADMT must be easy to execute, require minimal steps, and comply with section 7004; may not require a consumer to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer; and prohibits requiring a verifiable consumer request but permits a business to ask for information necessary to complete the request. The proposed regulations would allow a business to deny a request that it has a good-faith, reasonable, and documented belief is fraudulent, if it informs the requestor that it will not comply with the request and provides an explanation of why it believes the request is fraudulent. Consumers would be entitled to a means to confirm that their opt-out of ADMT request has been processed. The proposed regulations would permit a business to provide consumers with the choice of allowing specific uses of ADMT, so long as the business also offers a single option to opt-out of all ADMT subject to the proposed regulations. The proposed regulations would permit a consumer to submit requests using an authorized agent if the consumer provides signed permission to the agent. They would also allow a business to deny an authorized agent's request if the agent does not provide the signed permission to the business. Businesses would be required to wait at least 12 months before asking consumers that opted out of ADMT to consent to their use of that ADMT and prohibited from retaliating against consumers who exercised their right to opt-out of ADMT.

The proposed regulations would require that when a consumer has opted out of ADMT before the business initiated the processing, the business must not initiate processing of the

consumer's personal information using that ADMT. If a consumer submitted an opt-out of ADMT request after the business initiated the processing, the business would be required to cease processing the consumer's personal information using that ADMT as soon as possible, and no later than 15 business days after receiving the request. The proposed regulations would also prohibit the business from using or retaining any personal information previously processed by that ADMT and would require the business to notify all other persons to whom it disclosed information using that ADMT that the consumer has opted out and instruct them to comply with the opt-out within the same time frame.

The proposed regulations would add section 7222, which requires businesses to provide consumers with the ability to access information about the business's use of ADMT for significant decisions and extensive profiling, but does not require businesses using ADMT solely for training to provide a response to a consumer's request to access ADMT. The proposed regulations would clarify that businesses must provide a plain language explanation of the specific purpose for which the business used ADMT with respect to the consumer, and that this explanation must not describe the purpose in general terms. In addition, the business must provide a plain language explanation of the output of the ADMT with respect to the consumer. If the business has multiple outputs with respect to the consumer, the business would have the option to provide a simple and easy-to-use method for consumers to access those outputs. The proposed regulations would require a business to provide a plain language explanation of how the business used the output with respect to the consumer. For significant decisions, the proposed regulations would require the business to include the role the output played in the business's significant decision and the role of any human involvement, and how the business plans to use the output to make a decision. The proposed regulations would require that a business using ADMT for extensive profiling explain the role the output played in the evaluation that the business made with respect to the consumer; and if the business plans to use the output to evaluate the consumer, how the business plans to use the output to evaluate the consumer.

The proposed regulations would require the business to provide a plain language explanation of how the ADMT worked with respect to the consumer, including how the logic, including its assumptions and limitations, was applied to the consumer, and the key parameters that affected the ADMT and how they were applied to the consumer. Businesses would also be allowed to provide the range of possible outputs or aggregate output statistics, and an example of how to do so is provided. A business relying upon the security, fraud prevention, and safety exception is not required to provide information that would compromise its use of ADMT for security, fraud prevention, or safety purposes. The proposed regulations would also require that a business provide a plain language explanation to consumers that the business is prohibited from retaliating against consumers for exercising their CCPA rights, instructions for how the consumer can exercise their other CCPA rights, and any links to online request forms or portals for making such requests. The proposed regulations would also specify that the business cannot link the consumer to another section of the policy or to a place that requires the

consumer to scroll through other information. The proposed regulations would require that methods to submit request to access ADMT are easy to use and do not use dark patterns. Businesses would be allowed to use existing methods to submit requests to know, delete, or correct for requests to access ADMT.

The proposed regulations would require verification of the identity of the person making the request to access ADMT, and if a business cannot verify their identity, the business must inform the requestor that it cannot verify their identity. If a business denies a verified access request because of a conflict with other laws or an exception to the CCPA, the business would be required to inform the requestor and explain the basis of the denial, unless prohibited from doing so by law. If the request is denied only in part, the business would be required to disclose the other information sought by the consumer. The proposed regulations would require that businesses use reasonable security when transmitting the requested information to the consumer. Business would be allowed to maintain password-protected accounts with consumers to comply with a request to access ADMT by utilizing a secure self-service portal for consumers to access, view, and receive a portable copy of the requested information. The proposed regulations would require that the portal fully disclose the requested information that the consumer is entitled to receive about the business's use of ADMT with respect to them under the CCPA and these proposed regulations, utilize reasonable data security controls, and comply with the verification requirements.

The proposed regulations would require that service providers or contractors provide assistance to businesses in responding to verifiable consumer requests to access ADMT, including by providing personal information in their possession or enabling the business to access that information. The proposed regulations would clarify that businesses that use ADMT more than four times within a 12-month period with respect to a consumer may provide aggregate-level responses to a consumer's request to access ADMT and explain how information required in response to a request to access ADMT can be aggregated. The proposed regulations prohibit businesses from retaliating against a consumer for exercising their right to access ADMT.

The proposed regulations would require a business that uses ADMT to make an adverse significant decision concerning a consumer to provide the consumer with notice of their right to access ADMT as soon as feasibly possible and no later than 15 business days from the date of the adverse significant decision. An adverse significant decision would be a significant decision that resulted in a consumer being denied an educational credential; having their compensation decreased; being suspended, demoted, terminated, or expelled; or that resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services. The proposed regulations provide that a business must include in that notice: that the business used ADMT to make a significant decision with respect to the consumer; that the business is prohibited from retaliating against consumers for exercising their CCPA rights; that the consumer has a right to access ADMT and how the

consumer can exercise their access right; and, if applicable, that the consumer can appeal the decision and how they can submit their appeal and any supporting documentation. The proposed regulations would allow businesses to provide this notice to consumers with their notification of the adverse significant decision and provide an example. The proposed regulations would clarify that a business may provide this additional notice contemporaneously, to address instances where the business does not want to consolidate notices.

Article 12. Insurance Companies.

Article 12 would be a new article that contains requirements for insurance companies.

The proposed regulations would add section 7270, which defines the term "insurance company," pursuant to the California Insurance Code.

The proposed regulations would add section 7271 to clarify that insurance companies meeting the definition of "businesses" under the CCPA shall comply with the CCPA regarding any personal information collected, used, processed, or retained that is not subject to the California Insurance Code. The proposed regulations would acknowledge that the CCPA and Insurance Code may overlap in their jurisdiction and delineate the boundary between the two legal frameworks. By clarifying the circumstances under which the CCPA applies, the proposed regulations would allow insurance companies to evaluate how the CCPA would apply in situations where the Insurance Code does not apply. Illustrative examples are included.

Article 13. Investigations and Enforcement.

The proposed regulations would amend section 7300 by revising subsection (a) to replace "may" with "must" to clarify how consumers are to submit sworn complaints to the Agency.

The proposed regulations would amend 7302 to clarify that the Agency will provide the alleged violator with notice of the probable cause proceeding, and that a probable cause proceeding can be conducted in whole or in part by telephone or videoconference unless the alleged violator requests an in-person or public proceeding. An alleged violator would be able to request that the proceeding be in-person while also being closed to the public. Also, the proposed regulations clarify the proceedings may be held in whole or in part by telephone or videoconference. The proposed regulations would replace "participate or appear at" with "attend" and delete subsection (e).

Anticipated Benefits of the Proposed Regulations:

The proposed regulations provide a number of significant benefits to Californians, including both monetary and nonmonetary benefits.

The Agency's economic analysis revealed an anticipated decrease in monetary losses from the proposed regulations. Specifically, the Agency anticipates a reduction in cybercrimes—conservatively estimated to be approximately $1.5 billion in the first year of the proposed regulations' implementation and $66.3 billion in 2036. However, the primary benefits of the proposed regulations are not immediately calculable into dollars and cents, due to factors such as the abstract nature of privacy benefits, data and measurement limitations, variations in the privacy protections that businesses provide and in how they respond to regulations, and the fact that benefits can be long-term and take time to accrue to businesses, consumers, and society.

Despite the inability to translate the primary benefits of the proposed regulations into a monetary figure, they have widespread and profound societal benefits that further the purposes of the CCPA and honor the long history of privacy rights and business innovation in California. These important benefits include increased transparency and consumer control over personal information; reduced incidences of unauthorized actions related to personal information and harm to consumers; promotion of fairness and social equity; efficiencies, operational improvements, and competitive advantage for businesses; and the creation of new jobs and innovation.

Comparable Federal Regulations:

There are no existing federal regulations or statutes comparable to these proposed regulations.

Determination of Inconsistency/Incompatibility with Existing State Regulations:

As required by Government Code section 11346.5, subdivision (a)(3)(D), the Agency has conducted an evaluation of these proposed regulations and has determined that they are not inconsistent or incompatible with existing state regulations.

Forms or Documents Incorporated by Reference: None.

Other Statutory Requirements: None.

DISCLOSURES REGARDING THE PROPOSED ACTION

Agency's Initial Determinations:

Mandate on local agencies or school districts: None.

Cost or savings to any state agency: The Agency estimates that the proposed regulations will result in a one-time fiscal cost of $44,625 and ongoing fiscal costs of $129,035.

These costs result from the new workload for staff at the Agency and Department of Justice (DOJ). That workload includes (1) one-time staff work to build the frameworks necessary to receive required documents from more than 52,000 businesses and letters of complaint from an uncertain number of consumers; and (2) ongoing staff workload to review submitted documents and respond to submittals on a case-by-case basis.

The Agency's Information Technology Division will need to develop a web portal to accept the documents referenced above. Total one-time fiscal impact for creating this mechanism is estimated at $44,625. The ongoing fiscal costs of analyst and attorney staff to process this workload is estimated at $129,035.

Cost to any local agency or school district which must be reimbursed in accordance with Government Code sections 17500 through 17630: None.

Other non-discretionary costs or savings imposed on local agencies: None. Local governments are not subject to the proposed regulations because they do not meet the CCPA's definition of "business."

Cost or savings in federal funding to the state: None.

Cost impacts on representative private person or business: The compliance costs associated with the regulations will vary considerably depending on the type and size of business, the maturity of the business's privacy compliance system, the number of California consumers it services, and how it uses personal information. For a small business, initial costs are estimated at $7,045 to $92,896, with ongoing annual costs of $19,317. For a larger business, initial costs are estimated at $7,045 to $122,666, with ongoing costs of $26,015 annually. The Agency found no cost impact on consumers.

Significant effect on housing costs: None.

Significant, statewide adverse economic impact directly affecting businesses, including ability to compete:

The Agency has made an initial determination that the proposed regulations may have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states.

The Agency has considered proposed alternatives that would lessen any adverse economic impact on business and invites the public to submit proposals. Submissions may include the following considerations:

1. The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to businesses;
2. Consolidation or simplification of compliance and reporting requirements for businesses;
3. The use of performance standards rather than prescriptive standards; and
4. Exemption or partial exemption from the regulatory requirements for businesses.

The types of businesses that would be affected are businesses that that exceed $27,950,000.00 in revenue in the preceding calendar year; buy, sell, or share the personal information of 100,000 or more consumers or households per year; or receive 50% or more of their annual revenue from selling or sharing personal information. The proposed regulations may also affect service providers, contractors, and third parties that engage with businesses.

The projected reporting requirements include preparation and submission of a certification of completion of a cybersecurity audit, a certification of conduct of a risk assessment, and a risk assessment in abridged form.

To the extent that the proposed regulations restrict business activity of California businesses covered by the CCPA, the proposed regulations will impact the businesses' individual competitiveness against out-of-state competitors.

The Agency does not possess sufficiently detailed enterprise-level data to predict these competitive adjustments at the microeconomic level. However, its analysis—which focuses on supply, demand, and related estimates for the 2-digit NAICS sectors, mainly 51-Information and 52-Finance—indicates that California itself will not face significant percentage firm revenue and employment declines, which are generally in the low single-digit percentages of a more rapidly growing baseline trend (for example, a decrease of 0.47% in California supply and a decrease of 0.78% in investment, both relative to baseline in 2027).

With respect to out-of-state competition, as demand falls less than supply in a given year, some business will be diverted across California's border to available alternatives in other jurisdictions. However, the net slowing of growth for commerce remains modest. Relative

impacts (as a percentage of revenue) for the sector are more substantial than in comparison to the statewide economy, but they remain modest. For example, while the Agency estimates that there will be some sectoral diversion of business across California's border to available alternatives in other jurisdictions in 2027, it estimates that there will be an influx of business into California by 2031 and that the influx will increase substantially through 2036.

There are two basic structural adjustments in response to the proposed regulations. First, covered sectors will have to adjust to compliance costs, incurring higher labor costs in the short term and impinging on profit, investment, and capital in the medium term. The other salient impact comes from the demand side of the economy, as reductions in losses related to cybercrimes involving personal information leads to increases in real income for individuals and enterprises. These savings will be recycled through demand, stimulating the economy through traditional multiplier linkages. In California, 70% of aggregate demand comes from households and 70% of household consumption goes to services. In other words, 49% of the incremental benefits from reduced cybercrime losses will be channeled to demand for labor-intensive services, far outweighing the job losses due to compliance costs in more capital-intensive compliant sectors. Financial benefits eventually strongly overtake costs of the proposed regulations over the decade considered, but expenditure shifting to more labor-intensive activities makes these regulations even more pro-employment.

Results of the Standardized Regulatory Impact Assessment:

In the first 12 months following full implementation of the proposed regulation, the Agency estimates a direct impact of $3.5 billion in costs on the 52,326 businesses covered by the CCPA and affected by the proposed regulations, and $1.5 billion in quantified benefits. These direct costs and benefits may result in additional indirect and induced economic impacts. The total statewide costs of the proposed regulations are estimated to be $9.725 billion over the first 10 years following implementation. The quantified benefits are estimated to rise to $66.3 billion by 2036.

(1) The Agency anticipates the elimination of 98,000 jobs in the first 12 months following full implementation, followed by the addition of 233,000 jobs by 2036.

(2) The Agency does not anticipate that the proposed regulations would lead to the elimination of existing businesses. The proposed regulations are unlikely to eliminate existing businesses in California due to the threshold criteria for coverage and the size and type of businesses impacted. There is a possibility of some industry restructuring that could include a degree of consolidation of businesses that provide personal-information management services, but the Agency lacks information to assess the likelihood or potential for such a consolidation.

The Agency anticipates that the proposed regulations would lead to the creation of new businesses. The proposed regulations are likely to create new businesses in California

because of a significant increase in demand for labor with technical expertise in cybersecurity audits, risk assessment, automated decision-making technology, and consumer personal information privacy. The proposed regulations may create new businesses or new business lines that will help businesses, service providers, contractors, and third parties to comply with their obligations; and help consumers to understand and exercise their rights related to privacy.

(3) The Agency anticipates that the proposed regulations would put California businesses at a competitive disadvantage compared to businesses in other states during the first 12 months following full implementation of the proposed regulations. However, the Agency anticipates that the proposed regulations would put California businesses at a competitive advantage by 2031 and that that advantage would continue to increase through 2036.

(4) The Agency anticipates a decrease in investment in the state of $31 billion in the first 12 months following full implementation, followed by an increase in investment in the state of $261 billion by 2036.

(5) The Agency anticipates that the proposal would result in incentives for innovation in products, materials, or processes. Where existing practices are subject to restrictions, it is reasonable to expect firms will innovate and invest in product differentiation.

(6) The Agency anticipates the following benefits from the proposed action: The proposed regulations will enhance protection of consumer's personal information and increase the ability of individuals to exercise their privacy rights. Requirements to certify completion of risk assessments and cybersecurity audits will lead to reduced risks of cybercrimes against California businesses and individuals. Avoiding cybercrimes that involve consumers' personal information provides many types of benefits aside from financial measures as they include improvements to the health, safety, welfare, and quality of life for Californians.

Evaluating the cybersecurity risks with consumers' personal information and the effectiveness of cybersecurity systems set up to combat these risks helps inform firms about how to enhance the safety of consumers' information and privacy. The cybersecurity improvements that California businesses make help alleviate the social and psychological costs that cybersecurity threats impose on California consumers. Effective cybersecurity programs also lower the costs that cybercrimes create. The reduced costs of production and business activity can lower the price of goods and services that consumers pay. This lower cost of consumption together with more cybersecurity and privacy-protective business practices leads to improvements of consumer welfare.

In addition, the assessment of risks related to how businesses manage and protect personal information can lead to actions that help reduce those risks and improve safety within the workplace. Workers can focus their time and efforts on safety and efficiency, as they face

less burden in protecting consumer personal information, especially when businesses develop cybersecurity systems that mitigate risks and damages of cybercrimes.

Proposed requirements for training and uses of ADMTs will also provide benefits to businesses and individuals. Businesses that are required to evaluate their use of ADMTs will help ensure that the intended outcomes of those technologies are achieved, help improve efficiencies in the use of those ADMTs, and avoid a wide range of adverse outcomes associated with any of the unintended consequences of ADMTs implemented without such evaluations. The unintended consequences can include things like discrimination in both the hiring of employees and the provision of goods or services to consumers. Avoiding these adverse outcomes provides benefits in the workplace and to the health, safety, and welfare of California residents.

Business report requirement: The proposed regulations would require businesses that meet certain thresholds to submit reports to the Agency. If a business meets certain thresholds, it may be required to submit a certification of completion of its cybersecurity audit or a certification of conduct of its risk assessment and risk assessment in abridged form.

The Agency finds it is necessary for the health, safety or welfare of the people of this state that the reports be created and submitted by businesses. The certification of completion of a business's cybersecurity audit—together with Article 9's substantive requirements—is necessary to protect consumers' welfare. Specifically, it provides an assurance of, and accountability for, the thoroughness and independence of the business's audit, which will further protect consumers' personal information. Similarly, the certification of conduct of a business's risk assessment, and the submission of risk assessments in abridged form, are similarly necessary to protect consumers' welfare. In addition to fulfilling the CCPA's statutory mandate that risk assessments be submitted to the Agency on a regular basis, the certification of conduct of a business's risk assessment and the submission of risk assessments in abridged form provide assurances of, and accountability for, the business's risk assessments, which will further protect consumers' privacy.

Small business determination: The Agency has determined that the proposed action affects 6,915 to 27,659 small businesses.

Summary of Department of Finance Comments Regarding the Standardized Regulatory Impact Analysis and Agency Responses:

The Department of Finance provided comments on the Standardized Regulatory Impact Analysis ("SRIA") that addressed four issues relevant to the macroeconomic assessment and specifically requested additional clarification in those areas. Below is the Department of Finance's feedback, followed by Agency responses.

1. The SRIA should clearly identify the state revenue baseline used. The SRIA projects state tax revenue impacts to range from a decline of about $3 billion (or -0.13 percent, as stated in the SRIA) to an increase of $6 billion (0.3 percent) over the implementation period. However, these percentage estimates understate the projected state revenue impact, as $6 billion accounts for roughly 2 percent to 3 percent of the state's revenues, while the percentages estimated in the SRIA, imply a state revenue baseline of roughly $2 trillion.

   Response: Table 5.1 in Section 5.3 has been corrected – the BEAR Model results remain unchanged, but this table was constructed with incorrect baseline data for State and Federal revenues, which led to miscalculations of level and percent changes. These numbers have been revised in the table and reported in the text (e.g., in the paragraph preceding Table 5.1).

2. The SRIA is currently lacking critical disclosures and justification regarding impacts to the state's economy and budget including the following: 1) The estimated impact on Gross State Product (GSP) ranges from a decline of nearly $30 billion to an increase of $280 billion across the implementation period. Moreover, the ratio of GSP to state tax revenues averaged about 16- to-1 from 2017 to 2023, however, the projected ratio in the SRIA ranges from about 10-to-1 through 2031 before increasing significantly to 46-to-1 by 2036. The SRIA should further explain and justify the substantial change in the ratio of GSP to state revenues and why it is projected to rise significantly over the implementation period.

   Response: See response to item 1 above. These figures are now in agreement with DOF's notes related to baseline tax revenues and share of GSP. These modifications do not significantly alter the conclusions of the SRIA.

3. The SRIA describes the initial negative impact of the regulations on state investment as "small," at -5.5 percent of total state investment in 2027. Investment in all sectors (including those not directly affected by the regulation) across the state is subsequently projected to increase by $257 billion, or nearly 36 percent, by the end of the implementation period in 2036. The SRIA should explain why investment is assumed be this significantly impacted, both initially and cumulatively over the ten-year window.

   Response: The estimates of Direct Costs and Benefits exhibit a strong reversing trend from net cost to net benefit across the decade considered. Costs and benefits are structurally quite different and generally accrue to different stakeholders. While costs are incurred by the California businesses impacted by the proposed regulations, as set forth in Section 2, benefits are much more general and have been allocated across all sectors of the economy in proportion to value added. Other rules for targeting benefits could yield different microeconomic impacts, but there are no reliable predictions of the detailed incidence of cybercrime damages over the next decade, let alone patterns of cybercrimes averted by the proposed regulations. The main growth (investment, employment, etc.) drivers for these results are macroeconomic, however, driven by the

aggregate savings-investment constraint applied to baseline labor and capital allocation patterns.

We estimate that California businesses, as set forth in Section 2, incur costs, including increased labor costs and reduced profits and statewide saving. Impacted businesses increase spending on skilled labor, but the economy as a whole experiences lower aggregate savings, which with the BEAR Model's saving-investment balance necessarily reduces net investment.

Benefits are modeled as accruing across the entire economy (not only to impacted businesses) and represent savings from reductions in the subset of cybercrimes identified in Section 3. In the absence of detailed information about exact patterns of future cybercrime, these savings are allocated across all sectors in proportion to their value-added. In fact we do not know exactly who will experience the savings from reduced cybercrimes, but the cumulative savings are substantial (averaging $18.6B in annual avoided losses over the decade evaluated) and will support higher economywide investment levels through the same aggregate saving-investment balance. This leads to incremental and compounded average investment growth of about 3.1% annually and 34% over a decade. Admittedly, we optimistically assume the savings are reinvested in California, but this improvement in the investment climate is fully consistent with the intention of the proposed regulations to further protect consumers' privacy (including by protecting their personal information) and facilitate responsible innovation.

Note that this explanation has been added to Section 4.3 of the SRIA.

4. The SRIA projects employment to decline by up to 126,000 in 2030 before increasing by 241,000 by the end of the implementation period in 2036. As the proposed regulation is expected to disproportionately impact higher earners across the state in the information and professional, scientific, and technical services industries, which together account for about 10 percent of the state's total employment, the SRIA should discuss the disparate employment impacts by industry to the extent possible.

   Response: The disparate employment impacts by industry are described in Section 4.4 and 4.7 of the SRIA. Note that only the direct cost impacts will be concentrated in the "information and professional, scientific, and technical services" sectors and occupations. Most economywide effects, including direct benefits and all indirect and induced impacts will be dispersed across most economic activities and occupation categories (see response to Item 3 above). Even for the impacted businesses, there will be tradeoffs for skilled workers, between those hired to support compliance and those let go because of increased costs, and we lack prior information to predict this at the enterprise level.

For this reason, most occupations follow the aggregate adjustment process. The current version of the BEAR Model does detail 22 Standard Occupational Classification (SOC) 2-digit occupations and 60 sectors, but our fairly general assumptions about net benefit allocation do not shed much light on these detailed compositional effects.

Note that minor text changes have been made to Section 4.4 and a revised Table 4-3 has been added to Section 4.7 of the SRIA.

CONSIDERATION OF ALTERNATIVES

In accordance with Government Code section 11346.5, subdivision (a)(13), the Agency must determine that no reasonable alternative considered by the Agency or that has otherwise been identified and brought to the attention of the Agency would be more effective in carrying out the purpose for which the action is proposed, would be as effective and less burdensome to affected private persons than the proposed action, or would be more cost effective to affected private persons and equally effective in implementing the statutory policy or other provision of law. The Agency invites interested parties to submit alternatives with respect to the proposed regulations. The Agency's own alternatives to the proposed regulations are described in the Initial Statement of Reasons on pages 121–122.

CONTACT PERSONS

Inquiries concerning the proposed administrative action may be directed to:

Candice Sanders
California Privacy Protection Agency, Legal Division
2101 Arena Boulevard
Sacramento, CA 95834
(916) 642-7558
regulations@cppa.ca.gov

In the event the contact person is unavailable, inquiries regarding the proposed action may be directed to the following backup contact person:

Rianna Grenda
California Privacy Protection Agency, Legal Division
2101 Arena Boulevard
Sacramento, CA 95834
(279) 400-3449
Rianna.Grenda@cppa.ca.gov

AVAILABILITY OF STATEMENT OF REASONS, TEXT OF PROPOSED REGULATIONS, AND RULEMAKING FILE

The Agency will have the entire rulemaking file available for inspection and copying throughout the rulemaking process upon request to the contact person above. As of the date this Notice of Proposed Rulemaking is published in the Notice Register, the rulemaking file consists of this Notice, the Text of Proposed Regulations (the "express terms" of the regulations), the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based. The text of this Notice, the express terms, the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based are available on the Agency's website at https://cppa.ca.gov/regulations/ccpa_updates.html. Please refer to the contact information listed above to obtain copies of these documents.

AVAILABILITY OF CHANGED OR MODIFIED TEXT

After considering all timely and relevant comments, the Agency may adopt these regulations substantially as described in this Notice. If the Agency makes modifications which are sufficiently related to the originally proposed text, it will make the modified text, with the changes clearly indicated, available to the public for at least 15 days before the Agency adopts the regulations, as modified. Please send requests for copies of any modified regulations to the attention of the name and address indicated above. The Agency will accept written comments on the modified regulations for 15 days after the date on which they are made available.

AVAILABILITY OF THE FINAL STATEMENT OF REASONS

Upon its completion, a copy of the Final Statement of Reasons will be available on the Agency's website at https://cppa.ca.gov/regulations/ccpa_updates.html. Please refer to the contact information listed above to obtain a written copy of the Final Statement of Reasons.

AVAILABILITY OF DOCUMENTS ON THE INTERNET

Copies of this Notice, the express terms, the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based are available on the Agency's website at https://cppa.ca.gov/regulations/ccpa_updates.html.