CALIFORNIA PRIVACY PROTECTION AGENCY

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

FINAL STATEMENT OF REASONS AND UPDATED INFORMATIVE DIGEST

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, 7122, 7123, 7124, 7150, 7151, 7152, 7153, 7154, 7155, 7156, 7157, 7200, 7201, 7220, 7221, 7222, 7270, 7271, 7300, and 7302.

BACKGROUND

On November 22, 2024, the Agency issued a Notice of Proposed Rulemaking and began the 45-day comment period for proposed regulations containing updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies. ("CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.") In light of the Los Angeles wildfires' impact on the state and to ensure the opportunity to participate in this rulemaking for all Californians, the Agency extended the public comment period for this rulemaking to February 19, 2025. The Agency held virtual public comment hearings on January 14, 2025, and February 19, 2025. On May 9, 2025, the Agency issued a notice of modifications to text of proposed regulations and additional materials relied upon. The public comment period ended on June 2, 2025. After a review of all comments submitted on the proposed regulations, the Agency determined that no further substantive changes would be made to the proposed regulations and they were adopted by the Board on [insert date].

UPDATE TO INFORMATIVE DIGEST

Amendments to the CCPA went into effect on January 1, 2025. The amendments included: (1) the inclusion of "neural data" in the definition of "sensitive personal information"; (2) the inclusion of certain digital and physical formats of stored data, including artificial intelligence ("AI") systems that are capable of outputting personal information, in the definition of "personal information"; and (3) a requirement to comply with a consumer's pre-transfer preference to opt out from selling/sharing the consumer's personal information in case of a business transfer (such as a merger, acquisition or bankruptcy). Adjusted monetary amounts reflecting increases to the Consumer Price Index also went into effect on January 1, 2025.

None of these changes affect the substance of the proposed regulations that are the subject of this rulemaking. Where appropriate, the proposed regulations have been modified to be consistent with any change to the CCPA.

In response to public comments and further consideration, the Agency determined that there were several necessary sufficiently related modifications to the proposed regulations Specifically, those modifications are:

Article 1

§ 7001: The Agency deleted definitions for "artificial intelligence," "behavioral advertising," "deepfake," "publicly accessible place," and "zero trust architecture" because they were no longer necessary. The Agency added definitions for "cybersecurity audit report," "risk assessment report," and "sensitive location" to make clear what the modified regulations address. The Agency also moved the definition of "significant decision" to this section and modified the definition.

Similarly, the Agency modified the definitions for "automated decisionmaking technology," "information system," "nonbusiness," "physical or biological identification or profiling," "sensitive personal information," and "train."

§ 7002: In subsections (b)(2) and (c)(2), the Agency replaced the word "seeks" with "plans."

§ 7004: In subsection (a)(2)(D), the Agency added the words "equal or."

Article 2

§§ 7013 and 7014: In sections 7013, subsection (e)(3) and 7014, subsection (e)(3), the Agency made modifications to clarify when the notice to opt-out of sale/sharing and the notice to limit need to be provided.

Article 3

§ 7020: The Agency clarified the scope of personal information subject to the right to know.

§ 7022: The Agency deleted subsections regarding ensuring that information remains deleted.

§ 7023: The Agency deleted unnecessary words in subsection (c) and deleted subsections (f)(3) and (f)(6).

§§ 7023 and 7024: The Agency modified sections 7023, subsection (j) and 7024, subsection (d)(2), to provide an example of how a business could confirm that the personal information the business maintains is the same as what the verified consumer provides.

§ 7024: The Agency deleted subsection (e)(3).

§ 7026: The Agency modified this section to clarify in the example that this business can restrict the transfer of personal information immediately, and thus, must do so in response to a request to opt-out of sale/sharing.

§ 7027: The Agency modified subsection (m)(3) to add "or at consumers" to clarify that the right to limit exception also applies to actions directed at consumers.

§§ 7022, 7023, 7024, 7026, 7027: The Agency also deleted the requirement in sections 7022, subsection (g)(5), 7023, subsection (f)(6), 7024, subsection (e)(3), 7026, subsection (e), and 7027, subsection (f), that a business inform the consumer that they can file a complaint with the Agency and the Attorney General if they believe their privacy rights have been violated.

Article 4

§ 7050: The Agency modified subsections (h)(1) and (h)(2) to delete the phrases "as necessary for the auditor" and "in any manner." The Agency also added language

regarding information or facts "in a service provider's or contractor's possession, custody, or control."

Article 9

§ 7121: The Agency modified the title of this section to add "and Audit Reports." The Agency added subsection (a) to phase in implementation of the cybersecurity audit requirements between January 1, 2027 and April 1, 2030. The Agency also modified subsection (b) to address timing requirements for businesses after April 1, 2030.

§ 7122: The Agency modified subsection (a) to include examples of procedures and standards that are accepted in the profession of auditing, limit certain reporting, evaluation, and compensation requirements for businesses using internal auditors to the highest-ranking auditor, and remove the requirements for a business's board of directors or governing body.

The Agency modified subsection (b) to clarify examples of the purposes for which an auditor may request information. The Agency revised subsection (c) to delete the phrase "in any manner." The Agency modified subsection (d) and previous subsections (e)(1)–(4), (f), and (g) by removing the language specifying the content of a cybersecurity audit report and moving it to section 7123, subsection (e). The Agency modified subsection (e) to use the term "cybersecurity audit report" and add a cross reference to section 7123, subsection (e). The Agency modified subsection (f) to use the term "cybersecurity audit report" and remove the requirement that the cybersecurity audit be reported to the business's board of directors or governing body, and to instead require the cybersecurity audit report to be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program.

The Agency deleted previous subsection (i) to no longer require a signed certification by a member of the business's board or governing body. The Agency modified subsection (g), previously subsection (j), to clarify that the requirement to retain documents relevant to each cybersecurity audit applies to both the business and the auditor.

§ 7123: The Agency modified the title of this section to include "and Audit Report." The Agency modified subsections (a) through (d) to remove language about the content of a cybersecurity audit report, such as "document," "describe," and "identify." The Agency has consolidated the cybersecurity audit report requirements into subsection (e).

The Agency modified subsection (b) to move some requirements into subsections (e)(1) and (2), emphasize that the cybersecurity audit must assess the components of a cybersecurity program that the auditor deems applicable to the business's information system, delete certain documentation and explanation requirements, and add a cross-reference to subsection (c) to make it easier for businesses and their auditors to identify relevant components. The Agency also moved subsection (b)(3) up, deleted certain unnecessary phrases within this subsection, and clarified that the cybersecurity audit would also have to assess any additional components the business or auditor decided to include in the audit.

The Agency modified subsection (c) to add the term "if applicable" for the listed components that follow within this subsection. The Agency modified subsection (c)(1)(B), previously subsection (b)(2)(A)(ii), to clarify that the subsection would be applicable only if the business uses passwords or passphrases. The Agency deleted previous subsection (b)(2)(C) regarding "zero trust architecture." The Agency added the terms "account" and "application" to subsection (c)(3)(A), previously subsection (b)(2)(D)(i). The Agency modified subsection (c)(8)(A), previously subsection (b)(2)(I)(i), to clarify that bot-detection, intrusion-detection, and intrusion-prevention are examples of technologies that a business may use to detect and prevent unsuccessful login attempts, monitor the activity of authorized users, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information. The Agency also modified subsections (c)(12) and (13), previously subsection (b)(2)(M), to address cybersecurity awareness separately from cybersecurity education and training and move the phrase "how the business maintains current knowledge of changing cybersecurity threats and countermeasures" up to subsection (c)(12), which addresses cybersecurity awareness. The Agency modified subsection (c)(17)(A), previously subsection (b)(2)(Q)(i), to use the word "imminently" instead of "potentially" in the definition of "security incident" and add the word "personal" to focus on personal information.

The Agency modified subsection (e), previously subsection (c), to use the term "cybersecurity audit report" and consolidate the cybersecurity audit report requirements into this subsection. The Agency modified subsection (e)(1), previously section 7122, subsection (d), and subsection (b)(1), to clarify what the cybersecurity audit report must describe and explain, and replace the requirement to specifically identify and document the business's establishment, implementation, and maintenance of its cybersecurity program with a requirement to describe the business's information system and identify the policies, procedures, and practices

that the cybersecurity audit assessed. The Agency modified subsections (e)(2) and (e)(3), previously section 7122, subsections (e)(1)–(3), and subsection (c)(1), to consolidate and clarify the requirements relating to gaps or weaknesses in the business's cybersecurity program; delete the separate requirement to address the status of any gaps or weaknesses identified in any prior cybersecurity audit; modify the requirement that the cybersecurity audit report identify and describe in detail the status of any gaps or weaknesses, to instead have it address the gaps and weaknesses that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers' personal information; or unauthorized activity resulting in the loss of availability of personal information; remove the word "specifically" from the requirements; and require that the cybersecurity audit report also assess any additional component that the business or auditor decided to include in the audit.

The Agency modified subsection (e)(4) to no longer require that the cybersecurity audit document the resources allocated to address identified gaps and weaknesses in the business's cybersecurity program. The Agency also removed the word "specifically" from subsection (e)(5), previously section 7122, subsection (e)(4). The Agency modified subsection (e)(6), previously subsection (c)(4), to clarify that the business is not required to provide more than three titles of qualified individuals responsible for the business's cybersecurity audit program. The Agency modified subsection (e)(8), previously section 7122, subsection (g), to limit its requirements to the highest-ranking auditor. The Agency modified subsection (e)(10), previously section 7123, subsection (e), to no longer include language regarding notifications to other data processing authorities outside of California.

The Agency modified subsection (f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the requirements in Article 9, either on its own or by supplementation. The Agency also included an example of how a business may do so, and removed the requirement that a business specifically explain how the cybersecurity assessment work it is utilizing meets the requirements of Article 9.

§ 7124: The Agency modified subsection (a) to clarify that a business must submit a certification for each calendar year it is required to compete a cybersecurity audit. The Agency added subsection (b) to clarify when a business must submit its certification. Specifically, the Agency clarified that the business must submit its certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.

The Agency modified subsection (c) to clarify who must submit the certification and the requirements they must meet. The Agency modified this subsection to require that the certification be completed by a member of the business's executive management team who is directly responsible for the business's cybersecurity-audit compliance, has sufficient knowledge of the business's cybersecurity audit to provide accurate information, and has the authority to submit the business's certification to the Agency.

The Agency added subsection (d) to clarify how the business must submit its certification to the Agency and the information the certification must include. Specifically, this subsection requires that the certification include the business's name and the point of contact for the business; a statement that the business has completed the cybersecurity audit; the time period covered by the audit, by month and year; an attestation that the person completing the certification meets the requirements in the regulations and a certification under penalty of perjury that the information they submit is true and correct and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit; and the name and business title of the person submitting the certification and the date of the certification.

Article 10

§ 7150: The Agency modified subsection (b)(2)(A) to add an exemption for certain reasonable accommodations. It also moved the definition of "significant decision" to § 7001(ddd), removed the term "extensive profiling" in subsection (b)(3), which included removing the thresholds related to work or educational profiling, public profiling, and profiling for behavioral advertising. Subsections (b)(4) and (b)(5), previously subsections (b)(3)(B)(i) and (b)(3)(B)(ii), now address certain automated processing based upon (1) systematic observation of a consumer who is acting as an educational program applicant, job applicant, student, employee, or independent contractor for the business, or (2) a consumer's presence in a sensitive location. Subsection (b)(6), previously subsection (b)(4), now includes an intent standard and removes language regarding artificial intelligence, the generation of deepfakes, and the operation of generative models.

The Agency also revised the examples regarding when a business must conduct a risk assessment in subsection (c) to align with the changes to subsection (b), remove unnecessary language, and add further guidance in the examples.

§ 7151: The Agency modified subsections (a) and (b) to clarify which employees must be included in the risk assessment process, and that a business may include an external party in that process, with examples.

§ 7152: The Agency modified subsection (a) to remove the phrase "business must conduct and document" and add a new term, "risk assessment report." The regulations now clarify which portions of the risk assessment within section 7152, subsection (a), the business must document in its risk assessment report. The Agency provided examples regarding how to identify a purpose or benefit in non-generic terms in subsections (a)(1) and (a)(4). In addition, subsection (a)(2) now requires identification and documentation of categories of sensitive personal information and no longer includes requirements regarding the quality of personal information.

Subsections (a)(3)(B), (a)(3)(D), and (a)(3)(E) have been modified to include language such as "plans to," "if unknown," and "will be," to address circumstances where the processing will happen in the future or where the business may not yet know certain information. Subsection (a)(3)(C) now focuses on the business's method of interacting with consumers and the purpose of the interaction. Subsection (a)(3)(E) also references personal information to clarify the requirement for disclosures. Subsections (a)(3)(E) and (a)(3)(F) no longer require identification of certain actions a business has taken or plans to take, and subsection (a)(3)(G) no longer requires identification of the technology to be used in the processing beyond certain uses of ADMT.

The Agency also modified subsection (a)(4) to add the phrase "as applicable" when identifying benefits to the business, the consumer, other stakeholders, and the public, and remove language regarding a business's specific identification of monetary benefits.

The Agency modified subsection (a)(5) to remove the requirement regarding criteria used to make certain determinations, and further clarify that the list of negative privacy impacts are nonexhaustive. The Agency also modified the list of negative impacts within this subsection to use the term "protected characteristics" and delete the word "antidiscrimination"; provide additional guidance regarding dark patterns, economic harms, and reputational harms; delete duplicative negative impacts; use the word "would"; and delete unnecessary examples.

The Agency modified subsection (a)(6) to add language regarding the types of safeguards that must be identified and documented and clarify that the list of safeguards provided in this subsection is nonexhaustive. It also deleted the requirement regarding identification of how the safeguards address the negative impacts identified, and the requirement to identify certain evaluations and policies, procedures, and training when using ADMT. The regulations clarify that a business may consider implementing these policies, procedures, and training to ensure that the business's ADMT works as intended for the business's purpose and does not unlawfully discriminate based upon protected characteristics. The Agency also deleted language regarding evaluating the need for human involvement.

The Agency modified subsections (a)(8) and (a)(9) by clarifying who the relevant contributors, reviewers, and approvers are for a risk assessment; adding language regarding the relevant decisionmaker about whether the business will initiate the processing that is the subject of the risk assessment; and removing a requirement regarding the board of directors or governing body.

§ 7153: The Agency modified this section by removing references to artificial intelligence, limiting disclosure requirements to a business making ADMT available to another business to make a significant decision, and limiting the disclosure requirements to facts that are available to the business and necessary for the recipient-business to conduct its own risk assessment. The Agency also deleted previous subsection (b), which had additional disclosure requirements.

§ 7154: The Agency changed the title of this section to "Goal of a Risk Assessment." It also modified this section to state the goal of a risk assessment as stated in the CCPA.

§ 7155: The Agency modified subsection (a)(3)'s timing requirement for updates after a material change to as soon as feasibly possible, with an outer bound of 45 calendar days. It also removed language regarding diminishing benefits for material changes. The Agency also revised subsection (b), previously subsection (c) to provide a December 31, 2027, deadline for certain risk assessments and cross-reference relevant requirements in sections 7152 and 7157. Further, the Agency moved the retention requirements that were previously in subsection (b) to subsection (c).

§ 7156: The Agency modified subsection (a)(1) to reference the risk assessment report. It also modified subsection (b) to add language addressing how a business

may utilize a risk assessment prepared for another purpose to meet the requirements in section 7152. The Agency added subsection (b)(1) to provide an example of how a business can use a risk assessment that is compliant with another state law to comply with section 7152.

§ 7157: The Agency modified subsection (a) to provide April 1 deadlines for risk assessment submissions, depending on when the risk assessment was conducted. The Agency modified subsection (b) to revise the risk assessment information that must be submitted. Businesses must now submit the business's name and point of contact, with relevant contact information; the time period covered by the submission, by month and year; the number of risks assessments conducted and updated during the relevant time period, in total and for each processing activity identified in section 7150, subsection (b); whether the risk assessments conducted or updated involved the processing of each of the categories of personal information and sensitive personal information identified in the CCPA; an attestation that the business conducted a risk assessment for the relevant processing activities during the time period covered by the submission, and a certification under penalty of perjury that the information they submit is true and correct; and the name and business title of the person submitting the risk assessment information, and the date of the certification. The submission no longer requires a signature.

The Agency deleted previous subsections (b)(1)(iii), and (b)(2) through (b)(4), which would have required submission of abridged risk assessments.

The Agency also modified subsection (c)'s requirements for the individual who submits the risk assessment information to the Agency. The requirement has been revised to provide flexibility to businesses in selecting the relevant individual from their executive management team to submit the information, provided that the individual is directly responsible for risk-assessment compliance, has sufficient knowledge of the risk assessment to provide accurate information, and has the authority to submit the risk assessment information to the Agency.

Subsection (d), previously subsection (c), clarifies how the information must be submitted to the Agency. Lastly, subsection (e), previously subsection (d), extends the submission timeline for risk assessment reports to within 30 calendar days of the Agency's or the Attorney General's request.

Article 11

§ 7200: The Agency modified subsection (a) to focus on the use of ADMT for a significant decision. It also added subsection (b) to provide additional time for businesses to come into compliance with the ADMT requirements. Businesses must be in compliance no later than January 1, 2027. The Agency also moved the definition of significant decision from previous subsection (a)(1) to § 7001(ddd).

§ 7201: The Agency deleted this section regarding additional requirements for physical or biological identification or profiling.

§ 7220: The Agency modified subsection (a) to provide businesses with the ability to consolidate the Pre-use Notice with the notice at collection, provided that the notice at collection complies with subsections (b) and (c). The Agency also clarified when the Pre-use Notice must be presented to a consumer in subsection (b)(2). In addition, the Agency revised subsection (c) to clarify the information that must be in the Pre-use Notice, and provide additional guidance regarding how to describe the business's purpose for using the ADMT in non-generic terms, as well as the additional information the business must provide regarding how the ADMT works to make a significant decision and how the significant decision would be made if a consumer opts out. The Agency also removed references to training uses of ADMT, to align with the revised scope of this Article.

Further, the Agency modified subsection (d) to clarify that a business is not required to include trade secrets or certain information related to security, fraud prevention, or safety in the Pre-use Notice. The Agency also revised the examples in subsection (e) to align with the revised scope of Article 11 and provide additional guidance regarding how businesses can consolidate notices.

§ 7221: The Agency revised this section to reflect the revised scope of Article 11, which focuses on the use of ADMT to make a significant decision. The Agency also modified subsection (b), which addresses exceptions to the requirement to provide an opt-out of ADMT, by removing the security, fraud prevention, and safety exception; and clarifying what a business must do to qualify for the human appeal exception, and the exceptions for admission, acceptance, or hiring decisions and allocation/assignment of work and compensation decisions.

The Agency also modified subsection (c) to provide businesses with more flexibility when titling an opt-out link. Subsection (n) no longer includes unnecessary language regarding how to process an opt-out request and now clarifies which

ADMT the consumer has made a request to opt-out of, and therefore when the notification requirements in subsection (n)(2) are triggered.

§ 7222: The Agency revised this section to reflect the revised scope of Article 11, which focuses on the use of ADMT to make a significant decision. The Agency modified subsection (b) to clarify that a business needs to provide information about the logic of the ADMT and the outcome of the decisionmaking process for the consumer in response to the consumer's request to access ADMT. The Agency also modified subsection (b) to provide guidance regarding how to provide relevant information to the consumer.

The Agency also revised subsection (c) to clarify that a business is not required to include trade secrets or certain information related to security, fraud prevention, or safety when providing the information required by subsections (b)(2)–(3). The Agency also modified subsections (e) and (j), previously subsections (d) and(i), to add clarifying language regarding verification and remove unnecessary language, such as "key" and "generally."

The Agency also revised subsection (*l*), previously subsection (b)(4)(C), to clarify that businesses may provide additional information in response to a consumer's access ADMT request. Lastly, the Agency deleted previous subsection (k)'s notice requirement for adverse significant decisions.

Article 12

§ 7271: In subsection (b), the Agency deleted "and requirements" and added a third example to clarify how information subject to the Insurance Code would not be subject to the CCPA.

UPDATE TO INITIAL STATEMENT OF REASONS

Pursuant to Government Code section 11346.9, subdivision (d), the Agency hereby incorporates the Initial Statement of Reasons ("ISOR") prepared in this rulemaking. Unless a specific basis is stated for any modification to the regulations as initially proposed, the necessity for the adoption of new regulations as set forth in the ISOR continues to apply to the regulations as adopted.

All modifications from the initial proposed text of the regulations, including non-substantial changes, are summarized below. A "non-substantial change" is one that clarifies without materially altering the requirements, rights, responsibilities,

conditions or prescriptions contained in the original text. (Cal. Code Regs., tit. 1, § 40.) Unless specifically noted otherwise, all subsection references refer to the current subsection reflected in the final regulations text submitted to OAL in connection with this rulemaking package. All references to regulations are to Title 11 of the California Code of Regulations.

ARTICLE 1. GENERAL PROVISIONS

Amend § 7001. Definitions.

Subsection (c): The Agency deleted the definition of "artificial intelligence" because the Agency no longer uses the term "artificial intelligence" in the regulations. The CCPA and these regulations protect consumers' privacy and may apply to personal information processed by artificial intelligence whether stated expressly or not. Thus, the definition is not needed, and removal is necessary to maintain the regulations' internal consistency.

Subsection (e), previously subsection (f): The Agency modified the definition of "automated decisionmaking technology" or "ADMT" to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. This balances protections for consumer privacy and is necessary to simplify implementation for businesses at this time by reducing the types of technology that are in scope of the definition. The Agency modified the definition in response to public comments that recommended narrowing the definition to more closely align with how other jurisdictions address the use of ADMTs. These modifications support the Agency's efforts to harmonize with privacy laws in other jurisdictions while providing additional clarity and guidance for businesses. The Agency may revisit this definition in future rulemaking packages as necessary to further enhance consumer privacy protections.

The Agency also deleted the term "execute a decision" and the explanation of what "technology" includes for the purposes of the ADMT definition as unnecessary. The phrase "execute a decision" is duplicative with the existing language "replace human decisionmaking." The term "technology" does not need additional clarification because the "ADMT" definition already states that it must process personal information and use computation.

Subsection (e)(1): The Agency modified this subsection by replacing "substantially facilitate human decisionmaking" with "substantially replace human decisionmaking." The Agency also defined "substantially replace human

decisionmaking" as a business using the technology's output to make a decision without human involvement. The Agency further clarified that human involvement requires the human reviewer to know how to use and interpret the output, review it and other relevant information, and have the authority to make or change the decision made by the ADMT. These modifications are necessary to provide clarity for businesses so that they can determine whether their use of technology substantially replaces human decisionmaking and is therefore in scope of the definition of "ADMT."

Subsection (e)(3): The Agency changed the clause "provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking" to "provided that they do not replace human decisionmaking" to align with the other modifications the Agency made to subsections (e) and (e)(1). Those modifications include the Agency's deletion of "execute a decision" and "facilitate." The revised "provided that" language is also consistent with the regulations enacted by the California Civil Rights Council. (*See* Civil Rights Council, Final Unmodified Text of Proposed Employment Regulations Regarding Automated-Decision Systems, California Code of Regulations, title 2, Division 4.1, Chapter 5, Subchapter 2 (version 3/17/2025).) The Agency also deleted the illustrative examples as unnecessary at this time. These modifications are necessary to clarify for businesses that they cannot avoid complying with the requirements in Article 11 by configuring and using the listed technologies to make significant decisions without human involvement.

Previous subsection (g): The Agency deleted the definition of "behavioral advertising" because the Agency removed the corresponding "profiling for behavioral advertising" thresholds from Articles 10 and 11. This is necessary for the regulations' internal consistency.

Subsection (*l*): The Agency added the definition of "cybersecurity audit report" and used this term throughout Article 9 to clarify the information that must be included in a cybersecurity audit report that each business must create as part of its cybersecurity audit. This is necessary to provide clarity for businesses and their auditors, and to make the regulations easier to read and understand.

Previous subsection (n): The Agency deleted the definition of "deepfake" because the Agency removed the corresponding "generation of a deepfake" thresholds from Articles 10 and 11. This is necessary for the regulations' internal consistency.

Subsection (t), previously subsection (v): The Agency modified the definition of "information system" to focus on personal information. Specifically, the Agency clarified that the resources in scope of the definition are those that are organized for the processing of personal information or that can provide access to personal information. The Agency also added a sentence to clarify that the information system for which the business is responsible includes the use of a service provider's or contractor's resources. This is necessary to provide additional clarity for businesses and their auditors, including to assist in ensuring the appropriate scoping of a cybersecurity audit.

Subsection (v), previously subsection (x): The Agency modified the definition of "nonbusiness" to remove unnecessary words and make it easier to read and understand.

Subsection (ee), previously subsection (gg): The Agency modified the definition of "physical or biological identification or profiling" to clarify that this term includes automated measurement or analysis. The Agency also added a sentence to clarify that processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer is not in scope of the definition. This is necessary to provide additional clarity for businesses that non-automated measurements or analysis, and information that cannot identify or reasonably be linked with a consumer, are not in scope of this definition.

Previous subsection (*ll*): The Agency deleted the definition of "publicly accessible place" because the Agency removed the "profiling through systematic observation of a publicly accessible place" thresholds in Articles 10 and 11. This is necessary for the regulations' internal consistency.

Subsection (zz): The Agency added the definition of "risk assessment report" and used this term throughout Article 10 to clarify the information that must be included in a risk assessment report. This is necessary to provide clarity for businesses, and to make the regulations easier to read and understand.

Subsection (aaa): The Agency added the definition of "sensitive location" and used this term in section 7150, subsection (b)(5), to address the scope of the relevant risk assessment threshold. This definition identifies places where consumers are subject to significant privacy risks when they are subject to certain automated processing based on their presence in these locations. For example, consumers may not reasonably expect that visits to healthcare facilities or food pantries are

tracked and used to develop inferences about them. This is necessary to provide clarity to businesses and consumers about what locations are subject to certain requirements. This definition also incorporates feedback from public comments regarding locations that present discrete privacy issues or could reveal sensitive information about a consumer.

Subsection (bbb), previously subsection (ccc): The Agency modified the definition of "sensitive personal information" to add a consumer's neural data as a type of sensitive personal information to conform with recent changes to the CCPA. (S.B. 1223, Chapter 887 (Cal. 2024).)

Subsection (ddd), previously section 7150, subsection (b)(3)(A), and section 7200, subsection (a): The Agency has moved the definition of "significant decision" to section 7001 to make the regulations consistent and easier to read and understand. The Agency also modified the definition to provide additional clarity for businesses about the types of decisions that are in scope, and to further simplify implementation at this time by reducing the type of decisions that are in scope of this definition. Specifically, the Agency removed the terms "access to," "criminal justice," "insurance," and "essential goods and services" from the definition to simplify implementation for businesses at this time by reducing the type of decisions that are in scope of this definition. The Agency also removed cross-references to the CCPA's data-level exemptions as unnecessary, because the CCPA is reasonably clear in addressing which data are subject to the CCPA. The Agency may revisit this definition in future rulemaking packages as necessary to further enhance consumer privacy protections.

Subsections (ddd)(1)–(2) and **(5):** The Agency added definitions of "financial or lending services," "housing," and "healthcare services" to provide additional clarity for businesses about the types of decisions that are in scope. These definitions are responsive to public comments that sought more clarity on what these terms mean. These definitions draw from, and are consistent with, existing federal and California laws and regulations that similarly define these or similar terms. For example, the definition of "financial or lending services" is consistent with the California Consumer Financial Protection Law's definition of "financial product or service," which similarly addresses transmitting or exchanging funds and providing check cashing services. (*See* Fin. Code, § 90005(k).) The definition of "housing" is consistent with the California Civil Rights Council's housing discrimination regulations, which similarly define "housing accommodation." (*See* 2 Cal. Code Regs § 12005.) The definition of "healthcare services" is consistent with the Public Health

Service Act, which similarly defines "health care services." (*See* 42 U.S. Code § 234(d)(2).)

The Agency also clarified that a business's use of ADMT to provide or deny housing based solely on the availability or vacancy of the housing and successful receipt of payment for housing is not covered as a significant decision. This is necessary to clarify that this narrow use of personal information is not a significant decision and to simplify implementation for businesses by reducing the types of housing decisions that are in scope of the definition.

Subsections (ddd)(3) and **(4),** previously section 7150, subsections (b)(3)(A)(i) and (ii), and section 7200, subsections (a)(1)(A) and (B)**:** The Agency changed "includes" to "means," to clarify the scope of decisions for educational enrollment or opportunities and employment or independent contracting opportunities or compensation.

Subsection (ddd)(4)(B), previously section 7150, subsection (b)(3)(A)(ii)(2), and section 7200, subsection (a)(1)(B)(ii)**:** The Agency modified this subsection to clarify that "allocation or assignment of work" applies only to employees, to simplify implementation for businesses at this time by reducing the type of employment activities that are in scope of the definition.

Subsection (ddd)(6): The Agency clarified that a significant decision "does not include advertising to a consumer," to simplify implementation for businesses at this time by reducing the type of activities that are in scope of the definition.

The modified definition of "significant decision" is consistent with approaches taken in other jurisdictions, such as the General Data Protection Regulation and the Colorado Privacy Act, while furthering the purposes of the CCPA and providing clarity to businesses about which decisions are in scope. These modifications are necessary to simplify implementation for businesses at this time by reducing the type of decisions that are in scope of the definition, provide additional clarity for businesses, and make the regulations easier to read and understand.

Subsection (fff): The Agency modified the definition of "train" for the purposes of section 7150, subsection (b)(6), and section 7153, to address the revised training requirements in those sections. The Agency deleted "automated decisionmaking technology and artificial intelligence" from the defined term to align with the Agency's modifications to section 7150, subsection (b)(6). Keeping these terms in the definition of "train" is unnecessary because section 7150, subsection (b)(6), and

section 7153 already specify the technologies to which their requirements apply. Lastly, adding the cross-references to section 7150, subsection (b)(6), and section 7153 makes the regulations easier to read and understand.

Previous subsection (kkk): The Agency deleted the definition of "zero trust architecture" as unnecessary at this time because the Agency deleted the corresponding provision in section 7123 that used the term.

Non-substantial changes: The Agency also renumbered subsections and made non-substantial grammatical changes (adding commas) and other non-substantial changes (using "ADMT" instead of "automated decisionmaking technology," and deleting "of these regulations" as unnecessary).

Amend § 7002. Restrictions on the Collection and Use of Personal Information.

Subsections (b)(2) and (c)(2): The Agency replaced "seeks" with "plans." This change is necessary to provide additional clarity about the relevant personal information that the business plans to collect or process for purposes of section 7002, subsection (b)(2). Similarly, it is necessary to provide additional clarity about the relevant purpose for which the business plans to further collect or process personal information for purposes of section 7002, subsection (c)(2).

Amend § 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

Subsection (a)(2)(D): The Agency added "equal or" to the subsection. This is necessary to make clear that the choices should be equal or symmetrical and to be consistent with other subsections within this section.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

Amend § 7010. Overview of Required Disclosures.

Non-substantial changes: The Agency made non-substantial changes (using "ADMT" instead of "automated decisionmaking technology").

Amend § 7011. Privacy Policy.

Non-substantial changes: The Agency made non-substantial changes (using "ADMT" instead of "automated decisionmaking technology").

Amend § 7013. Notice of Right to Opt-out of Sale/Sharing and the "Do Not Sell or Share my Personal Information" Link.

Subsection (e)(3)(C): The Agency modified this subsection to include that a business can provide the notice of right to opt-out of sale/sharing "at the time" the connected device begins collecting the personal information. This is necessary to align the requirements of this notice with that of notices at collection. This benefits businesses by providing flexibility in how to provide the various notices required under the statute and allowing them to use one notice to meet both the notice at collection and notice of right to opt-out of sale/sharing requirements. It also benefits consumers by lessening notice fatigue and increasing the likelihood that the consumer will spend the time to read the notice.

Subsection (e)(3)(D): The Agency modified this subsection to include that a business can provide the notice of right to opt-out of sale/sharing either at the time the consumers enters the augmented or virtual reality environment, or before or at the time the consumer encounters the business within the augmented or virtual reality environment. This is necessary for the same reasons stated in subsection (e)(3)(C) above. It is also necessary to account for situations in which the consumer encounters the business for the first time within the virtual environment.

Amend § 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

Subsection (e)(3)(C): The Agency modified this subsection to include that a business can provide the notice of right to limit "at the time" the connected device begins collecting the personal information that it "uses or discloses for those purposes." Including "at the time" is necessary to align the requirements of this notice with that of notices at collection. This benefits businesses by providing flexibility in how to provide the various notices required under the statute and allowing them to use one notice to meet both the notice at collection and notice of right to limit requirements. It also benefits consumers by lessening notice fatigue and increasing the likelihood that the consumer will spend the time to read the notice. The phrase "uses or discloses for those purposes" is also necessary to clarify that the notice requirement applies to this specific right to limit.

Subsection (e)(3)(D): The Agency modified this subsection to include that a business can provide the notice of right to limit either at the time the consumers enters the augmented or virtual reality environment, or before or at the time the

consumer encounters the business within the augmented or virtual reality environment. This is necessary for the same reasons stated in subsection (e)(3)(C) above. It is also necessary to account for situations in which the consumer encounters the business for the first time within the virtual environment.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

Amend § 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.

Subsection (e): The Agency modified this subsection to include that the method described in the subsection is not required for personal information collected prior to January 1, 2022. This is necessary to conform the requirement with the language of the statute and make clear to businesses that information collected prior to January 1, 2022, is outside the scope of the statute for these requests to know.

Amend § 7022. Requests to Delete.

Subsections (b)(1), (c)(1), **(f)**, and **(f)(5)**, previously (g)(5)**:** The Agency deleted the last sentence of subsections (b)(1) and (c)(1) and the entirety of subsections (f) and (f)(5) to simplify implementation at this time. Public comments voiced concerns regarding how the provisions would be applied, as well as the cost of the provisions. The Agency has deleted them at this time for further evaluation.

Non-substantial changes: The Agency also renumbered subsections and made non-substantial grammatical changes (for example, changing semicolons to periods).

Amend § 7023. Requests to Correct.

Subsection (c): The Agency modified this subsection to delete "implement measures" in the first sentence because the words are redundant. This change is necessary to make the subsection simpler and easier to read.

Subsections (f)(3) and (f)(6): The Agency deleted these subsections to simplify implementation at this time.

Subsection (j): The Agency modified this subsection to provide an example of how a business could confirm that the personal information the business maintains is the same as what the verified consumer provides. This is necessary to clarify for

businesses how they can provide such a method and was included in response to public comments asking for more clarity.

Non-substantial changes: The Agency also renumbered subsections.

Amend § 7024. Requests to Know.

Subsection (d)(2): The Agency modified this subsection to provide an example of how a business could confirm that the personal information the business maintains is the same as what the verified consumer provides. This is necessary to clarify for businesses how they can provide such a method and was included in response to public comments asking for more clarity.

Subsection (e)(3): The Agency deleted this subsection to simplify implementation at this time.

Non-substantial changes: The Agency also renumbered subsections and made non-substantial grammatical changes.

Amend § 7026. Requests to Opt-out of Sale/Sharing.

Subsection (e): The Agency deleted the last two sentences of this subsection to simplify implementation at this time.

Subsection (f)(3)(A): The Agency modified this subsection to clarify in the example that this business can restrict the transfer of personal information immediately, and thus, must do so in response to a request to opt-out of sale/sharing. This clarification is necessary to address public comments about some instances in which a business using programmatic advertising technology cannot restrict the transfer of personal information instantly.

Amend § 7027. Requests to Limit.

Subsection (f): The Agency deleted the last two sentences of this subsection to simplify implementation at this time.

Subsection (m)(3): The Agency modified this subsection to add "or at consumers" to clarify that the right to limit exception also applies to actions directed at consumers. This is necessary to clarify that businesses can use sensitive personal information to protect consumers from malicious, deceptive, fraudulent, or illegal

actions. This exception balances protecting consumers' privacy with flexibility for businesses to protect themselves and consumers in limited circumstances.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

Amend § 7050. Service Providers and Contractors.

Subsections (h)(1) and (2): The Agency modified these subsections to delete the phrases "as necessary for the auditor" and "in any manner" as redundant and to make the regulations easier to read. Subsection (h)(1) already states that the service provider or contractor must make available to the auditor all relevant information that the auditor requests to complete the business's cybersecurity audit. Similarly, subsections (h)(1) and (h)(2) already prohibit the business from misrepresenting any fact relevant to the cybersecurity audit and any fact necessary to conduct the risk assessment, so retaining "in any manner" is unnecessary. Finally, the Agency added language regarding information or facts "in a service provider's or contractor's possession, custody, or control" to clarify the extent of their obligations. These modifications are necessary to improve the readability of the regulations and provide additional clarity for businesses, service providers, and contractors regarding which information or facts service providers and contractors must make available. These modifications help to ensure that businesses and their auditors have access to the information necessary to complete their cybersecurity audits and conduct their risk assessments even when the information relevant to their operations is in the possession of their service provider or contractor.

Non-substantial changes: The Agency made non-substantial changes to this subsection (deleting "by" and changing a semicolon to a comma).

Amend § 7051. Contract Requirements for Service Providers and Contractors.

Non-substantial change: The Agency made a non-substantial change to this section, by using "ADMT" instead of "automated decisionmaking technology."

ARTICLE 5. VERIFICATION OF REQUESTS

Amend § 7060. General Rules Regarding Verification.

Non-substantial changes: The Agency made non-substantial changes (using "notarized affidavit" instead of "notarization" and using "ADMT" instead of "automated decisionmaking technology").

ARTICLE 9. CYBERSECURITY AUDITS

Amend § 7121. Timing Requirements for Cybersecurity Audits and Audit Reports.

As explained in the ISOR, section 7121 is necessary to provide clarity to businesses regarding when they must comply with their statutory obligation to complete annual cybersecurity audits. It is also necessary to implement and operationalize the business's requirements to complete an annual cybersecurity audit. (*See* ISOR, p. 43.)

Title: The Agency modified the title of this section to add "and Audit Reports," to clarify that this section also addresses requirements for cybersecurity audit reports. This modification is necessary because section 7121 provides clarity for businesses about when they must complete their cybersecurity audit reports.

Subsection (a): The Agency added this subsection to: (1) phase in implementation by businesses' annual gross revenue over a three-year period, (2) clarify the audit period and specific date by which a business must complete its cybersecurity audit report, and (3) provide additional time after each audit period for businesses to complete their cybersecurity audit reports. These modifications are also responsive to public comments received during the formal public comment period. Comments sought additional time for businesses to come into compliance with Article 9 and sought additional time for businesses to complete cybersecurity audit reports following their completion of other cybersecurity auditing work. These modifications are necessary to simplify implementation for businesses by reducing their costs to comply with the regulations, provide clarity for businesses regarding when they must be in compliance, and provide businesses with more time to complete their cybersecurity audit reports.

Subsections (a)(1)–(3): The Agency added these subsections to phase in implementation by businesses' annual gross revenues. The Agency determined that businesses with higher annual gross revenues would be better able to bear the costs of earlier compliance. These subsections provide businesses that meet a criterion in section 7120 and have relatively lower annual gross revenues more time to complete their first cybersecurity audit and enable them to take advantage of learning and labor force developments in cybersecurity auditing. These modifications are necessary to reduce businesses' costs to comply with the regulations and to provide clarity for businesses regarding when they must comply

with their statutory obligation to complete annual cybersecurity audits. Specifically, **subsection (a)(1)** gives a business with more than one hundred million dollars in annual gross revenue until April 1, 2028, to complete its first cybersecurity audit. The Agency determined that giving such businesses well over a year from the anticipated effective date of the regulations to complete their first audit provided sufficient time for them to prepare for and come into compliance with the requirements. **Subsections (a)(2)–(3)** respectively give a business with between fifty million and one hundred million dollars in annual gross revenue more than two years from the anticipated effective date of the regulations to complete its first cybersecurity audit, and give a business with less than fifty million dollars in annual gross revenue more than three years from the anticipated effective date of the regulations to complete its first cybersecurity audit. The Agency determined that giving such businesses respectively over two and over three years from the effective date of the regulations to complete their first cybersecurity audits provided sufficient time for them to come into compliance.

Subsections (a)(1)–(3): For each of these subsections, the Agency also clarified the 12-month audit period and the specific date by which a business must complete its cybersecurity audit report. These modifications are necessary to provide clarity for businesses and to ensure that each cybersecurity audit is thorough. The Agency determined that April 1 — three months after each audit period ends (on January 1) — provides a business sufficient time to complete its cybersecurity audit report. The modifications clarify the specific date by which a business must complete its cybersecurity audit report after the audit period and are necessary to provide businesses with sufficient time to complete their cybersecurity audit reports. The April 1 deadline also provides consistency with the deadlines for a business's submission of its certification of completion of its cybersecurity audit and its risk assessments to the Agency. (*See* §§ 7124(b), 7157(a).) This benefits businesses by having a common deadline across the regulations.

Subsection (b): The Agency modified this subsection to clarify the cybersecurity audit period and the specific date by which a business must complete its cybersecurity audit report after April 1, 2030. This subsection addresses timing requirements for businesses after April 1, 2030, because subsection (a) phases in implementation for businesses that meet a criterion in section 7120 until April 1, 2030. The Agency added an illustrative example to provide further guidance for businesses so that they understand what their cybersecurity audit period will be, and the date by which they must complete their cybersecurity audit report. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure

that cybersecurity audits are thorough, provide clarity to businesses regarding when they must comply with their statutory obligation to complete annual cybersecurity audits, and provide businesses with sufficient time to complete their cybersecurity audit reports after the end of a cybersecurity audit period.

Amend § 7122. Thoroughness and Independence of Cybersecurity Audits.

Subsection (a): The Agency modified this subsection to delete "generally" from "generally accepted in the profession of auditing" as unnecessary because this subsection already requires auditors to use procedures and standards that are accepted in the profession of auditing. The Agency also added examples of procedures and standards that are accepted in the profession of auditing. The CCPA requires the Agency to establish a process to ensure that audits are independent. (*See* Civ. Code, § 1798.185(a)(14)(A).) These modifications are responsive to public comments that recommend the use of particular standards and are necessary to provide a flexible performative standard for businesses that provides them with guidance regarding how they must complete an independent cybersecurity audit.

Subsection (a)(1): The Agency added this subsection to clarify what it means to be a qualified auditor. Specifically, the subsection requires the auditor to have knowledge of cybersecurity and how to audit a business's cybersecurity program. This is necessary to provide a flexible performative standard for businesses that provides clarity regarding how they must complete an independent cybersecurity audit.

Subsection (a)(2), previously subsection (a)(1)**:** The Agency modified this subsection to delete the language "or appear to compromise" and to add the phrase "(separate from articulating audit findings)." The deletion is necessary to improve the clarity of this subsection about the auditor's obligations and to simplify implementation for businesses at this time. The added language is necessary to clarify that an auditor may make recommendations as part of articulating audit findings, which provide important information for a business to improve its cybersecurity, without compromising the auditor's independence.

Subsection (a)(3), previously subsection (a)(2)**:** The Agency modified this subsection to narrow the requirements' application to only to the highest-ranking auditor, to simplify implementation for businesses at this time by reducing the number of internal auditors for which businesses would have to implement the

reporting, evaluation, and compensation requirements of this subsection. For example, businesses engaging a team of internal auditors will not have to implement these requirements as to every internal auditor on the team. Retaining the requirements as to the highest-ranking auditor balances the benefits of supporting auditor independence and lessening the requirements for businesses. The Agency deleted the phrase "regarding cybersecurity audit issues" as unnecessary. The Agency also clarified that the goal of this subsection is to maintain the auditor's independence where the business uses an internal auditor. In addition, the Agency replaced the requirements that (1) the internal auditor report directly to the board of directors or governing body, and (2) the board or governing body conduct the auditor's performance evaluation and determine the auditor's compensation. The subsection instead requires a member of the business's executive management team, who does not have direct responsibility for the cybersecurity program, to fulfill those requirements. The Agency made these modifications in response to public comments that opposed mandatory board oversight of auditors and recommended requiring internal auditors to report to a business's highest-ranking executive without direct responsibility for the business's cybersecurity program. Finally, the Agency also added the phrase "if any" to clarify that businesses are not required to conduct performance evaluations of their auditors. These modifications are necessary to respond to public comments and provide further clarity to businesses regarding how to ensure that their cybersecurity audits are independent. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are independent. (*See* Civ. Code, § 1798.185(a)(14)(A).).

Subsection (b): The Agency deleted the first clause of this subsection and moved it to the end of the subsection to clarify that determining the scope of the cybersecurity audit and the criteria the cybersecurity audit will use are examples of the purposes for which an auditor may request information. As explained in the ISOR, this subsection is necessary because an audit cannot be thorough and independent unless the auditor has the information they deem necessary to make determinations about the scope of the audit and the criteria it will evaluate. (*See* ISOR, p. 45.)

Subsection (c): The Agency modified this subsection to delete "in any manner" as unnecessary because this subsection already prohibits the business from misrepresenting any fact relevant to the cybersecurity audit.

Subsection (d) and previous **subsections (e)(1)–(4), (f), and (g):** The Agency modified these subsections by removing the language specifying the content of a cybersecurity audit report and moving it to section 7123, subsection (e). The Agency consolidated the cybersecurity audit report requirements into section 7123, subsection (e), to make it easier for businesses and their auditors to identify what must be included in a cybersecurity audit report, and to distinguish the report requirements from the required components of the audit itself.

Subsection (d): The Agency modified the last sentence in this subsection to make the provision easier to read.

Subsection (e): The Agency modified this subsection to use the term "cybersecurity audit report" to clarify the information that must be included in a cybersecurity audit report. For clarity, the Agency also modified this subsection to add a cross reference to section 7123, subsection (e), which is where the Agency moved the language specifying the content of cybersecurity audit report.

Subsection (f), previously subsection (h)**:** The Agency modified this subsection to use the term "cybersecurity audit report" to clarify the information that must be included in a cybersecurity audit report. The Agency also modified this subsection to remove the requirement that the cybersecurity audit be reported to the board or governing body, and to instead require the cybersecurity audit report to be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program. These modifications are responsive to public comments that raised concerns about having to involve the business's board of directors. Requiring that senior individuals in the business responsible for its cybersecurity program be provided with the cybersecurity audit report helps to ensure that decisionmakers are informed about the business's cybersecurity posture, which furthers the intent and purpose of the CCPA to protect consumers' personal information. Knowing that the cybersecurity audit report will be reported to these individuals will likely motivate businesses to dedicate the appropriate resources and ensure that the cybersecurity audit will be of high quality. Retaining the requirement that the cybersecurity audit report be provided to a member of the business's executive management team, who has direct responsibility for the business's cybersecurity program, retains the benefit of ensuring that senior decisionmakers are informed about the business's cybersecurity posture, while lessening the compliance requirements for businesses. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent.

Previous subsection (i): The Agency deleted this subsection to simplify implementation at this time by lessening the requirements on businesses. Specifically, the regulations no longer require the cybersecurity audit to include a signed certification by a member of the business's board or governing body, certifying that the business made no attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit and that the signer reviewed and understands the audit's findings. The Agency added section 7124, subsection (d)(4), to retain the benefit of ensuring the cybersecurity audit's independence while lessening the compliance requirements for businesses. As explained in more detail below, section 7124, subsection (d)(4), requires the person completing the business's certification of completion to certify that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit. In combination with the auditor qualification and independence requirements in subsection (a), the prohibition against cybersecurity audit findings relying primarily on assertions or attestations by business management in subsection (d), and the requirements in subsections (b) and (c) that businesses make all relevant facts available to their auditors and that they must not misrepresent any such fact, these modifications balance ensuring the independence of the business's cybersecurity audit and lessening the compliance requirements on businesses.

Subsection (g), previously subsection (j)**:** The Agency modified this subsection to clarify that the requirement to retain documents relevant to each cybersecurity audit applies to both the business and the auditor. This modification is necessary because a business and its external auditor may generate and store different documents that are relevant to each cybersecurity audit, and businesses may use different external auditors over time. Specifying the duration that businesses and their auditors must retain documents relevant to cybersecurity audits is necessary to provide clarity to businesses and their auditors, and is necessary to enable the business to demonstrate compliance with the CCPA and these proposed regulations.

Non-substantial changes: The Agency renumbered the subsections and made other non-substantial changes (for example, deleting an extra "the").

Amend § 7123. Scope of Cybersecurity Audit and Audit Report.

Title: The Agency modified the title of this section to include "and Audit Report" to clarify that this section also addresses the requirements for cybersecurity audit

reports. This is necessary because section 7123 provides clarity for businesses about what they must include in their cybersecurity audit reports.

Subsections (a) through (d): The Agency modified these subsections to the remove language about the content of a cybersecurity audit report, such as "document," "describe," and "identify." The Agency has consolidated the cybersecurity audit report requirements into subsection (e). This is necessary to make it easier for businesses and their auditors to identify what must be included in a cybersecurity audit report.

Subsection (b)(1): The Agency modified this subsection to remove "including the components set forth in this subsection and subsection (b)(2)." The Agency moved this requirement to subsections (e)(1) and (2) to consolidate the cybersecurity audit report requirements into subsection (e). This is necessary to make it easier for businesses and their auditors to identify what must be included in a cybersecurity audit report.

Subsection (b)(2): The Agency modified this subsection to emphasize that the cybersecurity audit must assess the components of a cybersecurity program that the auditor deems applicable to the business's information system. This modification is responsive to public comments that seemed to misinterpret the subsection as requiring an audit to assess every component listed in subsection (b)(2), rather than assessing the "applicable" components. This modification is necessary to provide further clarity to businesses and their auditors about which components must be assessed. The Agency also deleted the requirement to document and explain why — when a component is not applicable — the component is not necessary and how the safeguards the business has in place provide at least equivalent security. This modification is responsive to public comments that raised concerns about having to address each component that is not applicable. This modification is necessary to simplify implementation for businesses at this time by lessening the documentation and explanation requirements for businesses and their auditors. Lastly, the Agency added a cross-reference to subsection (c) to make it easier for businesses and their auditors to identify the relevant components.

Subsection (b)(3): The Agency moved this subsection up to before the list of components to make the regulations clearer and easier to read. The Agency also deleted the phrases "at a minimum" and "including the safeguards the business identifies in its policies and procedures" as unnecessary. The phrase "at a minimum" is unnecessary because this subsection still requires the audit to assess how the

business implements and enforces compliance with its cybersecurity program, and section 7123, subsection (e)(2), requires the cybersecurity audit report to describe how the business implements and enforces compliance with its cybersecurity program. The phrase "including the safeguards the business identifies in its policies and procedures" is unnecessary because this subsection cross-references subsection (b)(1), which includes the written documentation related to the business's cybersecurity program, such as policies and procedures. Policies and procedures include safeguards for consumers' personal information, so it is not necessary to separately reference those safeguards. These modifications are necessary to provide clarity for businesses regarding what the audit must assess. The Agency also modified this subsection to clarify that the cybersecurity audit would also have to assess any additional components the business or auditor decided to include in the audit. This is necessary to provide further clarity to businesses and their auditors, and for consistency with subsection (d), which clarifies that an audit may assess components that are not set forth in subsections (b) or (c).

Subsection (c), previously (b)(2)**:** The Agency modified this subsection to further clarify that the audit must assess listed components of a cybersecurity program, "if applicable." Together with subsection (b)(2), this modification is necessary to provide clarity and guidance to businesses and their auditors, and to simplify implementation at this time.

Subsection (c)(1)(B), previously subsection (b)(2)(A)(ii)**:** The Agency modified this subsection to add "**I**f the business uses passwords or passphrases" to clarify that the subsection would be applicable only if the business uses passwords or passphrases. This modification is responsive to public comments and is necessary to provide clarity to businesses and their auditors.

Previous **subsection (b)(2)(C):** The Agency deleted the provision related to "zero trust architecture" to simplify implementation at this time by reducing the components that a business's cybersecurity must assess, if applicable.

Subsection (c)(3)(A), previously subsection (b)(2)(D)(i)**:** The Agency modified this subsection to add "account" and "application," because privileges and access may be granted to system or service accounts and applications, as well as to individual persons. These modifications are responsive to public comments and are necessary to provide clarity to businesses and their auditors.

Subsection (c)(8)(A), previously subsection (b)(2)(I)(i)**:** The Agency modified this subsection to clarify that bot-detection, intrusion-detection, and intrusion-prevention are examples of technologies that a business may use to detect and prevent unsuccessful login attempts, monitor the activity of authorized users, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information. This modification is responsive to public comments and is necessary to provide further clarity and guidance to businesses and their auditors.

Subsections (c)(12) and **(13),** previously subsection (b)(2)(M)**:** The Agency modified these subsections to make them easier to read and to address cybersecurity awareness separately from cybersecurity education and training. The Agency also moved the phrase "how the business maintains current knowledge of changing cybersecurity threats and countermeasures" up to subsection (c)(12), which addresses cybersecurity awareness, because the phrase pertains to cybersecurity awareness. These modifications are responsive to public comments that requested clarity regarding whether maintaining current knowledge of changing cybersecurity threats and countermeasures related to cybersecurity awareness or to cybersecurity education and training. These modifications are necessary to provide further clarity and guidance to businesses and their auditors.

Subsection (c)(17)(A), previously subsection (b)(2)(Q)(i)**:** The Agency modified this subsection to replace "potentially" with "imminently" in the definition of "security incident." This modified definition is consistent with how the National Institute of Standards and Technology ("NIST") defines "incident" in certain publications. The Agency also added "personal" to focus on personal information. These modifications are responsive to public comments and are necessary to provide clarity to businesses and their auditors, and to simplify implementation for businesses at this time.

Subsection (e), previously subsection (c)**:** The Agency modified this subsection to use the term "cybersecurity audit report" to clarify the information that must be included in a cybersecurity audit report. The Agency also consolidated the cybersecurity audit report requirements into this subsection. This is necessary to make it easier for businesses and their auditors to identify and understand what must be included in a cybersecurity audit report.

Subsection (e)(1), previously section 7122, subsection (d), and subsection (b)(1)**:** The Agency modified this subsection to clarify what the cybersecurity audit report must describe and explain, and to make it easier to read. The Agency has replaced the requirement to specifically identify and document the business's establishment, implementation, and maintenance of its cybersecurity program with a requirement to describe the business's information system and identify the policies, procedures, and practices that the cybersecurity audit assessed. These modifications are necessary to simplify implementation for businesses at this time by reducing their identification and documentation requirements, clarify what the cybersecurity audit report must articulate and explain, and make the regulations easier to read and understand.

Subsections (e)(2) and **(e)(3),** previously section 7122, subsections (e)(1)–(3), and subsection (c)(1)**:** The Agency modified these subsections to consolidate the requirements relating to gaps or weaknesses in the business's cybersecurity program and make the regulations easier to read and understand.

Specifically, the Agency deleted the separate requirement to address the status of any gaps or weaknesses identified in any prior cybersecurity audit as unnecessary, because the requirement that the cybersecurity audit report identify and describe in detail the status of any gaps or weaknesses already covers such gaps and weaknesses. The Agency also modified the requirement that the cybersecurity audit report identify and describe in detail the status of any gaps or weaknesses, to instead have it address the gaps and weaknesses that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers' personal information; or unauthorized activity resulting in the loss of availability of personal information. This is responsive to public comments that raised concerns about having to identify and describe every gap and weakness. This modification is necessary to simplify implementation at this time by requiring the cybersecurity audit report to address only those gaps and weaknesses that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers' personal information; or increase the risk of unauthorized activity resulting in the loss of availability of personal information. It is also necessary to provide additional clarity for businesses and their auditors about what the cybersecurity audit report must include.

The Agency also removed "specifically" to simplify implementation for businesses at this time by lessening the requirements for businesses. Finally, the Agency modified the requirements to clarify that the cybersecurity audit report must also

assess any additional component that the business or auditor decided to include in the audit. These modifications are necessary to simplify implementation at this time, clarify what the cybersecurity audit report must include, and make the regulations easier to read and understand.

Subsection (e)(4): The Agency modified this subsection to remove the requirement that the cybersecurity audit document the resources allocated to address identified gaps and weaknesses in the business's cybersecurity program. This modification is necessary to simplify implementation at this time by reducing businesses' documentation requirements.

Subsection (e)(5), previously section 7122, subsection (e)(4)**:** The Agency modified this subsection to remove "specifically." This is necessary to simplify implementation for businesses at this time by reducing their documentation requirements.

Subsection (e)(6), previously subsection (c)(4)**:** The Agency modified this subsection to clarify that the business is not required to provide more than three titles of qualified individuals responsible for the business's cybersecurity audit program, and to provide flexibility for businesses that have many individuals responsible for their cybersecurity programs. This is responsive to public comments and is necessary to simplify implementation for businesses at this time by reducing their documentation requirements.

Subsection (e)(8), previously section 7122, subsection (g)**:** The Agency modified this subsection to require only the highest-ranking auditor to sign and date the statement that certifies the independence of the audit, to provide flexibility for different businesses models, such as businesses that have teams of auditors conducting the business's cybersecurity audit. This is necessary to simplify implementation for businesses at this time by lessening the documentation requirements for businesses and their auditors.

Subsection (e)(10) previously section 7123, subsection (e)**:** The Agency modified this subsection to remove language regarding notifications to other data processing authorities outside of California. This is necessary to simplify implementation for businesses at this time by lessening their documentation requirements and to provide additional clarity for businesses and their auditors about what the cybersecurity audit report must include.

Subsection (f): The Agency modified this subsection in response to public comments that recommended that the Agency list cybersecurity frameworks and accept a business's use of them as compliant. The modifications that public commenters requested would not have been consistent with the CCPA, because a business's use of a cybersecurity framework is not necessarily an audit that would adhere to Article 9's thoroughness or independence requirements. Accordingly, the Agency modified this subsection to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the requirements in Article 9, either on its own or by supplementation. The Agency also included an example of how a business could utilize an audit that uses the NIST Cybersecurity Framework 2.0 and meets all of the requirements of Article 9. Additionally, the Agency removed the requirement that a business specifically explain how the cybersecurity assessment work it is utilizing meets the requirements set forth in the regulations. This modification is responsive to public comments that raised concerns about having to provide these explanations. These modifications are necessary to simplify implementation for businesses at this time by reducing their documentation requirements, and to provide additional clarity and guidance for businesses and their auditors.

Non-substantial changes: The Agency has renumbered subsections, made non-substantial grammatical changes (for example, replacing certain semicolons with commas or periods), and made other non-substantial changes (for example, updating cross-references, replacing an instance of "this includes" with "including," deleting an unnecessary instance of "as well as").

Amend § 7124. Certification of Completion.

Subsection (a): The Agency modified this subsection to clarify that a business must submit a certification for each calendar year it is required to compete a cybersecurity audit and to make it easier to understand. This is necessary to make the regulations easier for businesses and their auditors to understand and comply with.

Subsection (b): The Agency added this subsection to clarify when a business must submit its certification. Specifically, the Agency clarified that the business must submit its certification "no later than April 1 following any year that the business is required to complete a cybersecurity audit," which aligns with the modifications to section 7121 that require the business to complete its cybersecurity audit report no later than the same date. This is necessary to fulfill the Agency's statutory mandate

to establish a process to ensure that audits are thorough and independent, and to provide clarity to businesses about when they must submit their certification of completion to the Agency. It is also necessary to provide consistency with the deadlines for a business's completion of its cybersecurity audit report and submission of risk assessments to the Agency. (*See* §§ 7121, 7157(a).) This benefits businesses by having a common deadline for submissions across the regulations.

Subsection (c): The Agency modified this subsection to clarify who must submit the certification and the requirements they must meet, and to simplify implementation for businesses at this time by giving them flexibility in who completes the certification. These modifications are responsive to public comments that opposed requiring a member of the business's board to sign the business's certification of completion and certify that they reviewed and understand the findings of the cybersecurity audit. The Agency modified this subsection to require that the certification be completed by a member of the business's executive management team who is directly responsible for the business's cybersecurity-audit compliance, has sufficient knowledge of the business's cybersecurity audit to provide accurate information, and has the authority to submit the business's certification to the Agency. These modifications give businesses flexibility in selecting the relevant individual from their executive management team to submit the certification, while retaining the requirements that the person completing the certification has sufficient knowledge to provide accurate information. This is necessary to promote the integrity of information submitted to the Agency and to provide clarity to businesses about who must submit the certification to the Agency and the requirements they must meet. It is also necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent by providing accountability for the thoroughness and independence of the business's audit.

Subsection (d): The Agency added this subsection to clarify how the business must submit its certification to the Agency and the information the certification must include.

Specifically, the Agency added **subsection (d)(1)** to require that the certification include the business's name and the point of contact for the business. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent by providing accountability for the thoroughness and independence of the business's audit, and to enable the Agency

to link the certification to the business that submitted it and to contact the business about the certification.

The Agency added **subsection (d)(2)** to require the certification to include a statement that the business has completed the cybersecurity audit. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent, and to provide clarity to businesses about what their certification of completion to the Agency must include. This also ensures the Agency is able to monitor compliance with these cybersecurity audit requirements.

The Agency added **subsection (d)(3)** to require the certification to include the time period covered by the audit, by month and year. This requirement aligns with the modifications to section 7121 clarifying the audit period and the specific date by which a business must complete its cybersecurity audit report. This is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough, and to provide clarity to businesses regarding when they must comply with their statutory obligation to complete annual cybersecurity audits.

The Agency added **subsection (d)(4)** to require the person completing the business's certification of completion to attest that they meet the requirements in subsection (c), as well as certify under penalty of perjury that the information they submit is true and correct, and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit. Attestation that the person completing the certification meets the requirements in subsection (c) is necessary to fulfill the Agency's statutory mandate to establish a process that ensures audits are thorough and independent by providing accountability for the thoroughness and independence of the business's audit. Certification that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are independent. As explained in the ISOR with respect to previous section 7122, subsection (i), requiring the business to certify that the business made no attempt to influence the auditor's decisions or assessments is necessary to address the risks that businesses will seek to influence auditors' assessments of their cybersecurity posture. (*See* ISOR, p. 48.)

Certification under penalty of perjury helps to ensure that the certification of completion contains truthful, factual representations made in good faith. (*See e.g.,*

In re Marriage of Reese & Guy, 73 Cal. App. 4th 1214, 1223 (Cal. Ct. App. 1999), holding modified by *Laborde v. Aronson,* 92 Cal. App. 4th 459 (Cal. Ct. App. 2001) (explaining the use of certifications under penalty of perjury, "[t]he whole point of permitting a declaration *under penalty of perjury*, in lieu of a sworn statement, is to help ensure that declarations contain a truthful factual representation and are made in good faith").) Accordingly, the certification under penalty of perjury is necessary to ensure that businesses submit truthful and accurate information to the Agency. In addition, the certification under penalty of perjury helps ensure the reliability of the statements to the Agency since certifying under penalty of perjury can have a deterrent effect on those who may be considering not providing true, accurate, or complete information.

The Agency added **subsection (d)(5)** to require that the certification include the name and business title of the person submitting the certification and the date of the certification. This is necessary to enable the Agency to link the certification to the person who submitted it for the business, and to ensure accountability.

ARTICLE 10. RISK ASSESSMENTS

Amend § 7150. When a Business Must Conduct a Risk Assessment.

Subsection (b)(2)(A): The Agency modified this subsection to add the phrase "providing reasonable accommodation as required by law." This is necessary to limit the risk-assessment burden on businesses when processing sensitive personal information for routine personnel activities required by law. This also incorporates feedback received during the 45-day comment period on routine ways businesses may use sensitive personal information to provide reasonable accommodations for employees.

Subsection (b)(3): The Agency modified this subsection to remove the thresholds for "extensive profiling," and remove the definition "significant decision." Removing the "extensive profiling" term is necessary as the Agency moved the profiling thresholds addressing automated processing in the workplace, educational contexts, or sensitive locations to subsections (b)(4)–(5). Removing the "extensive profiling" term is necessary to avoid duplication in the subsection. In addition, the Agency removed one of the subparts of the extensive profiling definition, which addressed profiling a consumer for behavioral advertising, to simplify implementation for businesses at this time by reducing the amount of risk assessments they must conduct. This change is also responsive to public comments

that requested removal of the term "extensive profiling." Lastly, the Agency moved the "significant decision" definition to the "Definitions" section of the regulations. (*See* § 7001, subsection (ddd).) This is necessary to make the regulations consistent and easier to read and understand.

Subsection (b)(4), previously subsection (b)(3)(B)(i)**:** The Agency added this subsection to require a risk assessment for certain automated processing based upon systematic observation of a consumer who is acting as an educational program applicant, job applicant, student, employee, or independent contractor for the business. This threshold had previously been part of the "extensive profiling" definition in subsection (b)(3)(B)(i), which had addressed profiling through systematic observation more broadly. Moving this threshold to subsection (b)(4) is necessary to improve the readability of the regulations overall, as it provides a clear separate threshold from the significant decision threshold in subsection (b)(3). In addition, modifying this threshold to focus on automated processing to develop inferences or extrapolations about consumers in work or educational settings is necessary to clarify the types of automated processing that present significant risk to consumers' privacy in these settings. For example, consumers may not expect that automated tools in their workplace are developing inferences about their performance, reliability, or health. This change also simplifies implementation for businesses by focusing on specific types of automated processing, rather than on profiling more broadly.

Subsection (b)(5), previously subsection (b)(3)(B)(ii)**:** The Agency added this subsection to require a risk assessment for certain automated processing based upon a consumer's presence in a sensitive location. This threshold had previously been part of the "extensive profiling" definition in subsection (b)(3)(B)(ii), which had addressed profiling based upon systematic observation of a publicly available place. Moving this threshold to subsection (b)(5) is necessary to improve the clarity of the regulations, as it provides a clear separate threshold from the significant decision threshold in subsection (b)(3). In addition, modifying this threshold to focus on automated processing to develop inferences or extrapolations about consumers based on their presence in sensitive locations is necessary to clarify the types of automated processing that present significant risk to consumers' privacy. For example, consumers may not expect that their visits to healthcare facilities are tracked and used to develop inferences about their interest in specific types of medical treatment. This change also simplifies implementation for businesses by focusing on a specific types of automated processing, rather than on profiling more broadly. In addition, modifying this threshold to focus on sensitive locations

specifically, rather than on publicly available places more broadly, is necessary to simplify implementation for businesses at this time by reducing the scope of locations subject to this threshold. Sensitive locations address a discrete set of places where consumers are subject to significant privacy risks from automated inferences and extrapolations, such as healthcare facilities and places of worship. Narrowing this threshold also addresses feedback from public comments.

Lastly, this subsection excludes uses of personal information solely to deliver goods, or provide transportation for, a consumer at a sensitive location. This exclusion is necessary to clarify that these limited, routine uses of personal information do not create the types of inferences or extrapolations about consumers that would require a risk assessment.

Subsection (b)(6), previously subsection (b)(4)**:** The Agency modified this subsection to add an intent standard and remove the language regarding artificial intelligence, the generation of deepfakes, and the operation of generative models. The addition of the intent-based standard is necessary to clarify when a business using personal information for training purposes must conduct a risk assessment, and to simplify implementation for businesses at this time by limiting when they must conduct a risk assessment for these training uses. An intent-based standard is necessary to address some of the highest-risk training uses of personal information. It also addresses feedback from public comments requesting an intent-based standard. In addition, the definition of "intends to use" included in this subsection is necessary to clarify when businesses meet this standard, and addresses various actions that demonstrate a business's intent. Lastly, the removal of language regarding artificial intelligence, the generation of deepfakes, and the operation of generative models is necessary to simplify implementation for businesses at this time by reducing the scope of processing covered by this threshold.

Previous subsection (c)(1): The Agency deleted this example. This change is necessary because this example is duplicative with the example that follows, because both address the use of ADMT to make a significant decision.

Subsections (c)(1) through (c)(4), previously subsections (c)(2) through (c)(6)**:** The Agency modified these examples to replace "seeks" with "plans." Replacing "seeks" with "plans" is necessary for consistency and to provide additional clarity about when a business is required to conduct a risk assessment.

Subsection (c)(1), previously subsection (c)(2)**:** The Agency modified this example to add language regarding planning to videotape job interviews and lack of human involvement, and to remove language regarding physical or biological identification or profiling. The addition of language regarding videotaping job interviews that an emotion-recognition technology then uses to decide who to hire without human involvement is necessary to clarify how an ADMT can make a significant decision about a consumer. The addition of "without human involvement" is necessary to reflect the revised scope of the definition of ADMT, which focuses on technologies that replace or substantially replace human decisionmaking. Removing the phrase "specifically physical or biological identification or profiling" is necessary to avoid duplicative language in the example regarding the type of ADMT used.

Subsection (c)(3), previously subsection (c)(4)**:** The Agency modified this example to remove the phrase "conduct extensive profiling," and add the language "from their financial information." Removing the phrase "conduct extensive profiling" is necessary because the term "extensive profiling" was removed from the subsection (b)(3). Lastly, the addition of the term "from their financial information" is necessary to provide additional clarity in the example of how consumers' personal information can be used for sharing purposes.

Previous subsection (c)(5): The Agency removed this example. This change is necessary because the term "publicly accessible place" and its corresponding threshold in the definition of "extensive profiling" have been removed.

Subsection (c)(4), previously subsection (c)(6)**:** The Agency revised the example to replace the language regarding automated decisionmaking technology or artificial intelligence with the phrase "a facial-recognition technology." Using the phrase "a facial-recognition technology" is necessary to provide additional clarity regarding the type of technology being trained, and to align this example with the revised training threshold in subsection (b)(6).

Non-substantial changes: The Agency renumbered subsections and made other non-substantial changes (for example, replacing the word "automated decisionmaking technology" with the abbreviation "ADMT," and adding the word "follow" in subsection (c)).

Amend § 7151. Stakeholder Involvement for Risk Assessments.

Subsection (a): The Agency modified this subsection to clarify that employees whose job duties include participating in the relevant processing activity for a risk

assessment must be included in the risk assessment process, and to add an example of what type of employee must be included. This modification is necessary to further clarify which employees must participate in the risk assessment process, and to provide guidance about how an employee with relevant information for a risk assessment must provide that information to the individuals conducting the risk assessment. This helps to ensure risk assessments are thorough and comprehensive.

Subsection (b): The Agency modified this subsection to add language regarding utilizing or gathering information; replace "seeks" with "plans" and "involve" with "include"; and remove language regarding identifying, assessing, and mitigating risks. Adding language regarding utilizing or gathering information is necessary to clarify how a business may engage with relevant external parties when conducting a risk assessment. Replacing "seeks" with "plans" is necessary to provide clarity about when a business may want to utilize or gather information from a subset of consumers. Replacing "involve" with "include" is necessary to provide additional clarity about how external parties may be part of a risk assessment process. Removing language regarding identifying, assessing, and mitigating risks is necessary because a business may include external parties for other reasons when conducting a risk assessment, such as to obtain relevant facts.

Non-substantial changes: The Agency made non-substantial changes (for example, replacing the word "automated decisionmaking technology" with the abbreviation "ADMT").

Amend § 7152. Risk Assessment Requirements.

Subsection (a): The Agency modified the regulation to remove the phrase "business must conduct and document" and instead state that the risk assessment must include the requirements in this subsection. This change is necessary to clarify what the risk assessment must include and to improve the readability of the regulations. The removal of the word "document" is also necessary because a newly-added term, the "risk assessment report," clarifies which portions of the risk assessment within section 7152(a) must be documented.

Subsections (a)(1) through (a)(9): The Agency modified these subsections by removing the phrases "The business must" or "The business must specifically." This is necessary to avoid duplication in the regulations because subsection (a) already states that these elements must be in the risk assessment, and each subsection

identifies what is specifically required. In addition, the Agency added language regarding documentation in a risk assessment report in subsections (a)(1) through (a)(3), and (a)(6) through (a)(9). This is necessary to clarify which portions of a risk assessment must be documented. Subsections (a)(4) through (a)(5) no longer require documentation to simplify implementation for businesses at this time.

Subsection (a)(1): The Agency added an example of how to identify a purpose in non-generic terms. This is necessary to clarify how to identify a purpose with the necessary specificity to conduct a risk assessment.

Subsection (a)(2): The Agency removed the language "and whether they" and added "including any categories of" sensitive information. It also removed the requirements in what was previously subsection (2)(B) regarding the quality of personal information.

The modification regarding categories of sensitive personal information is necessary to clarify that a business must identify the specific categories of sensitive personal information to be processed, not just whether sensitive personal information will be processed. This is necessary because the type of sensitive personal information to be processed can affect the potential risks to consumers' privacy and relevant safeguards that a business may plan to implement. Lastly, removing subsection (2)(B) is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment. It is also responsive to public comments that requested removal of this requirement.

Subsection (a)(3)(B): The Agency modified this subsection to replace "will" and "used" with "plans to," and adding "if unknown" to clarify when a business must identify the criteria it plans to use to determine the retention period. Using the term "plans to" is necessary to clarify that the business must identify its planned retention period or the planned criteria to determine that retention period. Adding "if unknown" is necessary to clarify that a business must identify only the planned criteria to determine a retention period if the business does not know how long it plans to retain each category of personal information. This also addresses feedback from public comments that requested additional flexibility for businesses in complying with this requirement, by giving them the option to identify retention criteria if the business does not yet know the actual retention period.

Subsection (a)(3)(C): The Agency modified this section to focus on the business's method of interacting with consumers and the purpose of the interaction. This change is necessary to clarify the information that a business must identify about its interactions with a consumer to identify relevant risks and benefits as part of a risk assessment. Both the method and purpose of interaction can affect, for example, whether a consumer has meaningful control over their personal information, including whether the processing is consistent with their reasonable expectations. This change is also necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Subsection (a)(3)(D): The Agency modified this subsection to replace "seeks" with "plans." This change is necessary to provide additional clarity that the relevant information required for this subsection is what the business plans to process.

Subsection (a)(3)(E): The Agency modified this subsection by adding "of their personal information" and "will be," and deleting the last clause regarding actions the business has taken or plans to take. Adding "of their personal information" is necessary to clarify that the relevant disclosures to consumers are about the processing of their personal information. Adding "will be" is necessary because a business may not have made disclosures to a consumer regarding a planned processing activity at the time it is conducting a risk assessment, but will do so at a later time. Deleting the last clause is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Subsection (a)(3)(F): The Agency modified this section to delete the last clause regarding actions the business has taken or plans to take. Deleting the last clause is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Subsection (a)(3)(G): The Agency modified this subsection by deleting the first sentence regarding the technology to be used in the processing. The Agency also added "to make a significant decision" when addressing how the business will use the output of an ADMT. Deleting the first sentence is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment. Adding "to make a significant decision" is necessary to clarify that the business must identify how it

will use the output to make a significant decision about a consumer, which is the relevant processing activity for this operational element.

Subsection (a)(4): The Agency modified this subsection to add "as applicable," provide additional language regarding how to identify a benefit in non-generic terms, and remove the last sentence regarding a business's specific identification of monetary benefits. Adding "as applicable" is necessary to add flexibility for businesses, because a processing activity may only have benefits for a subset of the stakeholders identified, rather than all of them. Adding language regarding how to identify a benefit in non-generic terms is necessary to clarify how to identify a benefit with the necessary specificity to conduct a risk assessment. Lastly, removing the last sentence is necessary because it is duplicative with the first sentence of this subsection. If a business profits monetarily from a processing activity, this is a benefit to the business that must be identified in non-generic terms.

Subsection (a)(5): The Agency modified this section by removing the last clause regarding criteria used to make the determinations and adding "For example" to the prefatory sentence before the list of negative privacy impacts. Removing the last clause is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified for a risk assessment. Adding "For example" is necessary to clarify that this is a non-exhaustive list of examples for businesses to consider.

Subsection (a)(5)(B): The Agency modified this sentence to replace "protected classes" with "protected characteristics" and delete the word "antidiscrimination." The replacement is necessary for clarity, consistency, and harmonization with existing law. Deleting antidiscrimination is necessary because the relevant negative impact is unlawful discrimination, regardless of whether it is a law that is specifically labelled as an antidiscrimination law.

Subsection (a)(5)(D): The Agency modified this sentence to add an example of how consent cannot be freely given because it was obtained through the use of a dark pattern. This example is necessary to provide additional clarity and guidance on how a business could fail to obtain freely given consent.

Previous subsection (a)(5)(E): The Agency deleted this subsection because it is redundant with impairing consumers' control over their personal information, which is a negative impact to consumers' privacy already set forth in subsection (a)(5)(C).

For example, a business that discloses a consumer's media consumption without providing sufficient information for the consumer to make an informed decision about the disclosure is impairing consumers' control over their personal information.

Subsection (a)(5)(E), previously subsection (a)(5)(F)**:** The Agency modified this subsection by adding "based upon profiling." This addition is necessary to provide additional guidance of how economic harms can result from processing a consumer's personal information.

Subsection (a)(5)(G), previously subsection (a)(5)(H)**:** The Agency modified this subsection by changing "would" to "could," adding language to the dating application example regarding stigmatization for disclosures outside of the dating application, and deleting language regarding other examples. Changing "would" to "could" is necessary to clarify that these are possible negative impacts to an average consumer. Adding language for the dating application example is necessary to clarify how reputation harms, such as stigmatization, can occur for disclosures that consumers would not reasonably expect, such as disclosing their sexual or other preferences outside of a dating application. The Agency deleted the other examples because they are not necessary for additional clarity at this time.

Subsection (a)(5)(H), previously subsection (a)(5)(I)**:** The Agency modified this subsection by changing "would" to "could," deleting the example regarding targeting certain consumers with alcohol advertisements, and adding the word "disclosure" to the last example. Changing "would" to "could" is necessary to clarify that these are possible negative impacts to an average consumer. The Agency deleted the example because it is not necessary for additional clarity at this time. Adding the word "disclosure" is necessary to improve readability of the regulations, so it is clear that emotional distress can result from disclosure of a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

Subsection (a)(6): The Agency added language regarding the types of safeguards that must be identified and documented, and deleted the last sentence regarding identifying how the safeguards address the negative impacts identified. The addition regarding the types of safeguards identified, such as safeguards to address the negative impacts identified in subsection (a)(5), is necessary to clarify that businesses are not limited to identifying only those safeguards that address identified negative impacts when conducting a risk assessment. Deleting the last

sentence regarding how the safeguards address the negative impacts is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Subsection (a)(6)(A): The Agency modified this subsection by adding "For example" to the prefatory sentence before the list of safeguards. Adding "For example" is necessary to clarify that this is a non-exhaustive list of examples for businesses to consider.

Previous subsection (a)(6)(A)(iv): The Agency deleted this subsection. The definition of ADMT has been modified to exclude those uses that include human involvement. The removal of this example regarding evaluating the need for human involvement is necessary to address the revised scope of ADMT uses that require a risk assessment.

Subsection (a)(6)(A)(iv), previously subsection (a)(6)(B)(ii)**:** The Agency revised this subsection to address implementing policies, procedures, and training to ensure that the business's ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. This modification is necessary to clarify that this is a type of safeguard that a business may consider when conducting a risk assessment. Lastly, changing "protected classes" to "protected characteristics" is necessary for clarity, consistency, and harmonization with existing law.

Previous subsection (a)(6)(B): The Agency deleted the requirement that businesses identify certain evaluations and policies, procedures, and training when using ADMT as set forth in section 7150, subsection (b)(3). This is no longer a requirement to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Subsection (a)(8): The Agency modified this subsection by changing "contributors" to "individuals who provided information" and adding language excluding legal counsel who provided legal advice from this requirement. The Agency also deleted the last clause regarding maintaining the information in a separate document and the individuals within the business and external parties who contributed to the risk assessment.

Changing "contributors" to "individuals who provide information" is necessary to provide additional clarity regarding which individuals must be identified and documented for this requirement. Adding language regarding legal counsel is

necessary to clarify that businesses are not required to include attorneys who provided legal advice for the risk assessment. Lastly, removing the final clause is necessary because it is redundant with the new language. It is not necessary to have language regarding maintaining this information in a separate document, because it must be documented in a risk assessment report. Nothing prohibits a business from keeping this information elsewhere. In addition, it is not necessary to say "individuals within the business and external parties" because this requirement already states that businesses must identify the individuals who provided the information for the risk assessment.

Subsection (a)(9): The Agency modified this subsection by adding language regarding which individuals who reviewed or approved the risk assessment, excluding legal counsel; adding language regarding which decisionmaker must be part of the review and approval of the risk assessment; and removing the last sentence regarding the board of directors and governing body.

Adding language regarding who reviewed and approved the risk assessment is necessary to clarify that only the individuals who actually reviewed and approved the risk assessment must be identified and documented. Adding language regarding legal counsel is necessary to clarify that businesses are not required to include attorneys who provided legal advice to review and approve the risk assessment. Adding language regarding who must review and approve the risk assessment is necessary to clarify that this must be an individual with authority to participate in deciding whether the business will initiate the processing activity. This addresses circumstances where more than one person is the decisionmaker for a processing activity. Lastly, removing the last sentence regarding the board of directors and governing body is necessary to simplify implementation for businesses at this time by reducing the amount of information that must be identified and documented for a risk assessment.

Non-substantial changes: The Agency renumbered the subsections and made other non-substantial changes (for example, replacing the word "automated decisionmaking technology" with the abbreviation "ADMT," capitalizing certain words, using "a" instead of "the").

Amend § 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology.

Subsection (a): The Agency modified this subsection to delete the term "artificial intelligence," replace "for any processing activity" with "to make a significant decision," update the corresponding cross-reference to section 7150, subsection (b)(3), and add that the facts must be available to the business. Deleting the term "artificial intelligence" and limiting the requirement to the use of ADMT for significant decisions in section 7150, subsection (b)(3) is necessary to simplify implementation for businesses at this time by reducing the scope of processing subject to the disclosure requirements. In addition, adding the phrase "available to the business" is necessary to clarify the information a business's obligation extends to, and that it does not include information that is unavailable to the business.

Previous subsection (b): The Agency deleted this subsection to simplify implementation for businesses at this time by reducing their disclosure obligations.

Subsection (b): The Agency modified this subsection to remove the reference to "artificial intelligence." This modification is necessary because the Agency removed the artificial intelligence-specific disclosure requirement in subsection (a), so it is unnecessary to include it in subsection (b).

Non-substantial changes: The Agency renumbered subsections and made other non-substantial changes (for example, replacing the word "automated decisionmaking technology" with the abbreviation "ADMT").

Amend § 7154. Goal of a Risk Assessment.

The Agency changed the title of this section to "Goal of a Risk Assessment." This is necessary to clarify the goal of a risk assessment as stated in the CCPA.

Subsection (a): The Agency has modified this subsection to state the goal of a risk assessment as stated in the CCPA. (*See* Civ. Code § 1798.185(a)(14)(B).) This is necessary to provide the statutory goal of a risk assessment in the regulations, so that the requirements and goal are in one place. This improves the clarity and readability of this Article overall.

Amend § 7155. Timing and Retention Requirements for Risk Assessments.

Subsection (a)(3): The Agency modified this subsection to replace "immediately" with "as soon as feasibly possible, but no later than 45 calendar days from the date of the material change." It also removed the language regarding diminishing benefits. The timing change is necessary to provide clarity to businesses regarding when a risk assessment must be updated, with an outer bound of 45 calendar days. The Agency selected 45 days as the outer bound because this provides time for businesses to consult with relevant employees about the material change and its impact on the processing activity's negative impacts and safeguards, and update their risk assessments accordingly. This timeline is also consistent with other CCPA requirements, which use a similar 45-day timeline. (*See, e.g.*, § 7021(b).) This balances protections for consumer privacy with providing flexibility for businesses in meeting their compliance obligations. The removal of the benefits language is necessary to simplify implementation of the update requirements at this time by reducing the circumstances when a business must update a risk assessment after a material change.

Subsection (b), previously subsection (c)**:** The Agency revised this subsection to add "as set forth in section 7152," provide a calendar date by which risk assessments subject to this subsection must be completed, and cross-reference the submission requirements in section 7157, subsection (a)(1). Adding "as set forth in section 7152" is necessary to clarify that a business must conduct and document a risk assessment in compliance with the requirements in that section. Providing a calendar deadline is necessary to provide clarity to businesses about the date by which they must be in compliance with this subsection's requirements. The Agency chose December 31, 2027, as the calendar deadline because the Agency anticipates this will be approximately 24 months after the approval date of the regulations, which is consistent with the originally proposed requirement. Lastly, the cross-reference to the submission requirements in section 7157, subsection (a)(1) is necessary to provide clarity regarding the relevant submission requirements for the risk assessments subject to this subsection.

Subsection (c), previously subsection (b)**:** The Agency moved what was previously subsection (b) to subsection (c). This change is necessary to improve the readability of section 7155, which now provides timing requirements in subsections (a) and (b), followed by the retention requirement in subsection (c).

Non-substantial changes: The Agency renumbered the subsections.

Amend § 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

Subsection (a)(1): The Agency modified this subsection by replacing "and document" with "including documenting required information in its risk assessment report." This change is necessary to align with the revised requirements in section 7152, and to clarify that part of conducting a risk assessment includes documenting relevant portions of it in a risk assessment report.

Subsection (b): The Agency modified this subsection by adding language addressing how a business may utilize a risk assessment prepared for another purpose to meet the requirements in section 7152. The revised language also states that the risk assessment must contain the information that must be included in, or be paired with the outstanding information necessary for, compliance with section 7152. This revised language is necessary to provide a clear standard for when businesses may use other risk assessments, such as those prepared to comply with other laws, to comply with the requirements in section 7152. It is also necessary to prevent businesses from trying to use a risk assessment that is not as thorough or privacy-protective as one conducted in compliance with section 7152. This provision enables businesses to leverage existing compliance processes while ensuring they meet the requirements in the CCPA and these implementing regulations. It benefits businesses by providing them with flexibility and reducing their burden when operating in multiple jurisdictions.

Subsection (b)(1): The Agency added this subsection to provide an example of how a business can use a risk assessment that is compliant with another state law to comply with section 7152. This example is based on the Colorado Privacy Act regulations for data protection assessments, which overlap significantly with the requirements in section 7152. This example is necessary to clarify and provide guidance to businesses about how to utilize and supplement a risk assessment conducted for another purpose to meet the requirements in section 7152.

Amend § 7157. Submission of Risk Assessments to the Agency.

Subsection (a)(1): The Agency modified this subsection to provide a calendar date, April 1, 2028, by which businesses must submit risk assessment information for risk assessments conducted in 2026 and 2027. This modification is necessary to clarify

when information must be submitted. The calendar date, April 1, 2028, was chosen to provide businesses with additional time to prepare relevant risk assessment information for submission to the Agency, and to provide flexibility for businesses to come into compliance for their first submission.

Subsection (a)(2): The Agency modified this subsection to provide an annual calendar date by which a business must submit risk assessment information for risk assessments conducted after 2027. The calendar date, April 1, was chosen because it provides businesses with additional time each submission year to prepare relevant risk assessment information for submission to the Agency. It also is necessary to provide consistency with the deadlines for a business's completion of its cybersecurity audit report and certification of completion of its cybersecurity audit. (*See* §§ 7121, 7124(b).) This benefits businesses by having a common deadline across the cybersecurity audit and risk assessment regulations. The example provided is necessary to provide additional guidance to businesses about the timing of submissions.

Subsection (b): The Agency modified this subsection to revise the risk assessment information that must be submitted.

Specifically, the Agency added **subsection (b)(1)** to require that the submission include the business's name and point of contact, including the contact's name, phone number, and email address. This is necessary to enable the Agency to link the submission to the business that submitted it and to contact the business about the submission, and to align with the cybersecurity audit certification requirements.

The Agency modified **subsection (b)(2)**, previously subsection (b)(1)(B)(i), to require that the submission include the time period covered by the submission, by month and year. This is necessary for the Agency to identify when a business conducted the relevant risk assessments.

The Agency modified **subsection (b)(3),** previously subsection (b)(1)(B)(i), to require that the submission include the number of risks assessments conducted and updated during the relevant time period, in total and for each processing activity. This is necessary for the Agency to identify how many risk assessments businesses conducted each year and which processing activities triggered more or less risk assessments. This enables the Agency to fulfill its statutory mandate under Civil Code section 1798.199.40, subdivision (e), which requires the Agency to provide a public report summarizing risk assessments filed with the Agency while ensuring

that data security is not compromised. In addition, this is necessary for the Agency to identify whether businesses would benefit from additional guidance for conducting risk assessments for certain processing activities, which is consistent with the Agency's statutory mandate to provide guidance to businesses regarding their duties and responsibilities under Civil Code section 1798.199.40, subdivision (f).

The Agency added **subsection (b)(4)** to require that the submission include whether the risk assessments conducted or updated involved the processing of each of the categories of personal information and sensitive personal information identified in the CCPA. This is necessary for the Agency to identify what categories of personal information and sensitive personal information are involved in the processing activities that require a risk assessment. This enables the Agency to fulfill its statutory mandate under Civil Code section 1798.199.40, subdivision (e), which requires the Agency to provide a public report summarizing risk assessments filed with the Agency while ensuring that data security is not compromised. In addition, this is necessary for the Agency to identify whether businesses would benefit from additional guidance for conducting risk assessments involving certain categories of personal information and sensitive personal information, which is consistent with the Agency's statutory mandate to provide guidance to businesses regarding their duties and responsibilities under Civil Code section 1798.199.40, subdivision (f).

The Agency revised **subsection (b)(5)**, previously (b)(1)(B)(ii), to require that the submission include an attestation that the business conducted a risk assessment for the relevant processing activities during the time period covered by the submission. The attestation also requires that the person submitting it meets the requirements of section 7157, subsection (c). Lastly, it requires that the person declare under penalty of perjury that the risk assessment information submitted is true and correct.

Businesses no longer are required to have a designated executive certify that they have reviewed, understood, and approved all of the business's risk assessments. However, they must submit an attestation with the higher-level information described above. This balances simplifying implementation for businesses at this time while ensuring accountability at the highest levels of the business for risk assessments.

Further, certification under penalty of perjury helps to ensure that the certification of completion contains truthful, factual representations made in good faith. (*See,*

e.g., In re Marriage of Reese & Guy, 73 Cal. App. 4th 1214, 1223 (Cal. Ct. App. 1999), holding modified by *Laborde v. Aronson*, 92 Cal. App. 4th 459 (Cal. Ct. App. 2001) (explaining the use of certifications under penalty of perjury, "[t]he whole point of permitting a declaration *under penalty of perjury*, in lieu of a sworn statement, is to help ensure that declarations contain a truthful factual representation and are made in good faith").) Accordingly, the certification under penalty of perjury is necessary to ensure that businesses submit truthful and accurate information to the Agency. In addition, the certification under penalty of perjury helps ensure the reliability of the statements to the Agency since certifying under penalty of perjury can have a deterrent effect on those who may be considering not providing true, accurate, or complete information. Lastly, this requirement is also necessary to align with the cybersecurity audit certification requirements.

The also Agency modified **subsections (b)(6)**, previously subsection (b)(1)(iv), to require that the submission include the name and business title of the person submitting the risk assessment information, and the date of the certification. The submission no longer requires a signature to simplify implementation for businesses at this time by reducing the amount of information required as part of the submission.

Previous **subsections (b)(1)(iii), and (b)(2) through (b)(4)** have been deleted to simplify implementation for businesses at this time by reducing the amount of information a business must prepare for its annual submission. This modification addresses feedback from public comments that requested further reducing the time and resources a business expended to prepare its submission. The revised risk assessment information, including the certification, provides the Agency with necessary information to assess whether the risk assessment regulations are being implemented by businesses and to provide a public report summarizing risk assessments filed with the Agency, while ensuring that data security is not compromised. (*See* Civ. Code, § 1798.199.40(d).)

Subsection (c): The Agency modified this subsection to identify the requirements for the individual who submits the risk assessment information to the Agency. This requirement was previously in subsection (b)(1)(A), but has been moved to subsection (c) to improve readability. The requirement has also been revised to provide flexibility to businesses in selecting the relevant individual from their executive management team to submit the information, provided that the individual is directly responsible for risk-assessment compliance, has sufficient knowledge of the risk assessment to provide accurate information, and has the authority to

submit the risk assessment information to the Agency. This revision is necessary to provide additional flexibility for businesses in risk assessment submissions, by enabling them to choose whoever meets this subsection's requirements within their executive management team to submit the information. It also is necessary to ensure accuracy in risk assessment submissions, by requiring that individuals at the highest levels of the business are accountable for providing the necessary information to the Agency.

Subsection (d), previously subsection (c)**:** The Agency modified this subsection to replace "materials" with "information." This modification is necessary for consistency with the language used in subsections (a)–(c), which uses the term "risk assessment information." The Agency also deleted the title of this subsection, "Method of Submission," as redundant with the requirements of this subsection.

Subsection (e), previously subsection (d)**:** The Agency modified this subsection to require submission of risk assessment reports within 30 calendar days of a request by the Agency or Attorney General. These revisions are necessary to specify that the actual risk assessment report must be submitted to the Agency or Attorney General upon request. In addition, the change from "10 business days" to "30 calendar days" is necessary to simplify implementation for businesses at this time by extending their time period for submission. The Agency selected 30 calendar days because it is consistent with the Colorado Privacy Act regulations' analogous submission requirement, which promotes interoperability for businesses operating across both states. This modification also addresses public comments that requested additional time to submit this information to the Agency. Lastly, the Agency deleted the title of this subsection, "Risk Assessments Must Be Provided to the Agency or to the Attorney General Upon Request," as redundant with the requirements of this subsection.

Non-substantial changes: The Agency renumbered the subsections and made other non-substantial changes (for example, using "via" instead of "through").

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

Amend § 7200. When a Business's Use of Automated Decisionmaking Technology is Subject to the Requirements of This Article.

Subsection (a): The Agency modified this subsection to include the phrase "uses ADMT to make a significant decision concerning a consumer" to clarify when

businesses must comply with the requirements of Article 11. The Agency modified this subsection in response to public comments that recommended narrowing the uses of ADMT that would require a business to comply with ADMT requirements, including to more closely align with how other jurisdictions address the use of ADMTs. These modifications support the Agency's efforts to harmonize with privacy laws in other jurisdictions while providing additional clarity for businesses. These modifications are necessary to simplify implementation for businesses at this time, and to provide clarity for businesses as to when their use of ADMT is subject to the requirements of Article 11. The Agency may revisit this threshold in future rulemaking packages as necessary to further enhance consumer privacy protections.

Previous subsection (a)(1): The Agency moved and modified the definition of "significant decision" to section 7001, subsection (ddd)**.** This is necessary to make the regulations consistent and easier to read and understand.

Previous subsections (a)(2) through (3): The Agency deleted these subsections, to align with the modified definition of ADMT. This is necessary for clarity and consistency within the regulations.

Subsection (b): The Agency added this subsection to provide a calendar date by which businesses must be in compliance with the requirements in Article 11. The Agency made this modification to provide businesses with additional time to comply with the ADMT requirements after the effective date of the regulations, while ensuring that consumers could exercise their rights to opt-out of ADMT and to access ADMT no later than January 1, 2027. This modification is in response to public comments requesting additional time for businesses to come into compliance with the ADMT requirements in Article 11. The Agency selected January 1, 2027, because the Agency anticipates this will be approximately 12 months after the approval date of the regulations. This gives businesses sufficient time to build out or adapt their compliance processes for processing opt-out and access ADMT requests. This is necessary to simplify implementation for businesses at this time and to provide clarity to businesses regarding when they must comply with their statutory obligation to provide consumers with access and opt-out rights with respect to businesses' use of ADMT.

Non-substantial changes: The Agency also made non-substantial changes (for example, using "ADMT" instead of "automated decisionmaking technology").

Delete § 7201. Requirement for Physical or Biological Identification or Profiling.

The Agency deleted this section to simplify implementation for businesses at this time by reducing the mandatory evaluation and safeguarding requirements that businesses must comply with. A business that uses ADMT for a significant decision must still conduct a risk assessment and comply with opt-out and access ADMT requirements.

Amend § 7220. Pre-use Notice Requirements.

Subsection (a): The Agency modified this subsection to add language clarifying that a business may provide a Pre-use Notice in its notice at collection, provided that the notice at collection complies with, and includes the information required by, subsections (b) and (c). This modification provides a flexible, performance-based standard for businesses regarding how to provide the required information, while ensuring that consumers have meaningful information about the business's use of ADMT with respect to them when they are exercising their CCPA rights. This is necessary to provide clarity and guidance to businesses regarding how to provide the required information. It also incorporates feedback from public comments requesting additional flexibility for businesses to consolidate a Pre-use Notice and a notice at collection.

Subsection (b)(2): The Agency modified this subsection to clarify when a business must provide a Pre-use Notice to a consumer. Specifically, the Agency modified this subsection to clarify that a business must provide a Pre-use Notice at or before the point when the business collects the consumer's personal information that it plans to process using ADMT. This modification is consistent with the requirement that a business provide a notice at collection at or before the point of collection. (§ 7012, subsection (a).) The Agency also added a sentence to clarify that when a business has already collected a consumer's personal information for a different purpose and subsequently plans to process it using ADMT, the business must provide the consumer with a Pre-use Notice before processing their personal information for that purpose. This addition is consistent with the existing requirement regarding when a business must provide a new notice at collection. (*See* § 7012, subsection (f).) These modifications are necessary to provide clarity to businesses about when they must provide a Pre-use Notice, and to enable consumers to make informed choices about whether and how to exercise their rights to opt-out of and access ADMT before the business processes their personal information.

Subsection (c)(1): The Agency modified this subsection to add further clarity regarding why generic terms are not helpful for consumers in disclosures, and to modify the example of a generic term so that it aligns with the modifications the Agency made to section 7200, subsection (a). This is necessary to provide further clarity and guidance for businesses regarding the information they must include in Pre-use Notices, for the regulations' internal consistency, and to prevent businesses from using vague language about their planned use of ADMT, which undermines consumers' exercise of their rights to opt-out of and access ADMT. In addition, the Agency replaced "proposes" with "plans" to provide additional clarity about when a business must provide an explanation of the specific purpose for which it plans to use ADMT.

Previous subsections (c)(1)(A), (c)(3)(A), and (c)(5)(D): The Agency deleted these subsections to align with the modifications the Agency made to section 7200, subsection (a), which no longer include the separate threshold regarding training uses of ADMT. These modifications are necessary for the regulations' internal consistency and to simplify implementation for businesses at this time.

Subsection (c)(5): The Agency modified this subsection to clarify that a business must include in the Pre-use Notice how the ADMT works to make a significant decision about consumers and how the significant decision would be made if a consumer opts out. These modifications are necessary to provide additional clarity for businesses regarding what information they must disclose to consumers, and to simplify implementation at this time. Specifically, this information provides consumers with concise and clear disclosures about how a business plans to use ADMT to make a significant decision concerning them, while reducing the granularity of information the business is required to provide.

Subsection (c)(5)(A): The Agency modified this subsection to require that businesses provide information about how the ADMT processes personal information to make a significant decision about consumers, including the categories of personal information that affect the output generated by the ADMT. This is necessary to provide a flexible, performance-based standard for businesses regarding how to provide the required information, and to provide additional clarity on what information must be included in the Pre-use Notice. This information is necessary to ensure that consumers understand how the ADMT would process their personal information, so they can decide whether to opt-out of or access more information about that use of their personal information. The Agency also modified the subsection to add that an output may include decisions and to remove that

output includes "content," because the former is a clearer term for businesses to understand. These modifications are necessary for the regulations' internal consistency, to simplify implementation at this time by reducing the granularity of the information that businesses must disclose, and to provide clarity and guidance for businesses regarding what information they must disclose to consumers.

Subsection (c)(5)(B): The Agency modified this subsection to clarify what a business must include in the Pre-use Notice, specifically the type of output generated by the ADMT and how the business uses the output of the ADMT to make a significant decision. This is necessary to provide consumers with information regarding how the ADMT's output will be used to make a significant decision concerning them, so they can decide whether to opt-out of or access more information about that use of their personal information. The Agency also added an example of how a business could explain how it uses the output of the ADMT to make a significant decision, noting that the explanation may include whether the output is the sole factor or what the other factors in the business's decisionmaking process are, and a human's role in the decisionmaking process, if any.

These modifications are necessary to provide further clarity and guidance for businesses about what information is relevant for consumers to exercise their rights, and provide consumers with the most meaningful pieces of information necessary to inform consumers' decisions about whether to exercise their rights to opt-out of and access ADMT. The modifications also make the regulations easier to read and understand.

Previous subsection (c)(5)(B)(i): The Agency deleted this subsection as unnecessary in light of the modifications the Agency made to subsection (c)(B)(5). This modification is necessary for the regulations' internal consistency.

Previous subsection (c)(5)(B)(ii): The Agency deleted this subsection to align with the modifications the Agency made to section 7200, subsection (a), which no longer include a separate threshold for profiling for behavioral advertising. This modification is necessary for the regulations' internal consistency.

Section (c)(5)(C): The Agency modified this subsection by deleting the subsection that pertained to a business relying upon the security, fraud prevention, and safety exception, to align with the Agency's deletion of previous section 7221, subsection (b)(1). This is necessary for the regulations' internal consistency. The Agency added the requirement that the business explain what the alternative process for making a

significant decision is for consumers who opt out, in response to public comments suggesting this addition. This modification is necessary to ensure that consumers have meaningful factual information necessary to inform their decisions about whether to exercise their rights to opt-out of and access ADMT, such as what happens if they decide to opt-out.

Subsection (d): The Agency added this subsection to clarify that a business is not required to include trade secrets or certain information related to security, fraud prevention, or safety when providing the information required by subsection (c)(5). This is necessary to provide further clarity for businesses regarding what information they must disclose to consumers, and give businesses flexibility regarding how they can comply with the Pre-use Notice requirements while providing appropriate protections from public disclosure for trade secrets or certain security, fraud prevention, and safety information.

Subsection (e)(1), previously subsection (d)(1)**:** The Agency modified this subsection to clarify that the example pertains to a business's use of ADMT to make two different significant decisions concerning a consumer. This modification aligns with the modifications the Agency made to the definitions of "ADMT" and "significant decision" and to the scope of this Article, which specifically addresses the use of ADMT to make a significant decision concerning a consumer. It is necessary for the regulations' internal consistency, to simplify implementation at this time by reducing the number of notices a business must provide, and to provide further clarity and guidance for businesses regarding how they can consolidate Pre-use Notices.

Subsection (e)(2), previously subsection (d)(2)**:** The Agency modified this subsection to clarify that the example pertains to a business's use of multiple ADMTs to make a single significant decision concerning a job applicant. This modification aligns with the revised definitions of "ADMT" and "significant decision" and the revised the scope of this Article, which specifically addresses the use of ADMT to make a significant decision concerning a consumer and no longer includes public profiling. It also uses the term "job applicant" instead of consumer to provide additional clarity regarding when a business may be using multiple ADMTs for a single purpose, in this case to make a significant decision regarding who the business will hire. These modifications are necessary for the regulations' internal consistency, to simplify implementation at this time by reducing the number of notices a business must provide, and to provide further clarity and guidance for businesses regarding how they can consolidate Pre-use Notices.

Subsection (e)(3), previously subsection (d)(3)**:** The Agency modified this subsection to clarify that the example pertains to a business's use of multiple ADMTs to make multiple significant decisions concerning a consumer. This modification aligns with the revised definitions of "ADMT" and "significant decision" and the revised scope of this Article, which specifically addresses the use of ADMT to make a significant decision concerning a consumer and no longer includes the use of ADMT to grant access to secured classrooms. In this example, the relevant significant decisions are whether a student is suspended and granted a diploma or certificate. This modification is necessary for the regulations' internal consistency, to simplify implementation at this time by reducing the number of notices a business must provide, and to provide further clarity and guidance for businesses regarding how they can consolidate Pre-use Notices.

Subsection (e)(4), previously subsection (d)(4)**:** The Agency modified this subsection to clarify that the example pertains to a business's systematic use of ADMT to make significant decisions concerning a consumer. This modification aligns with the revised definition of "significant decision," which limits the allocation or assignment of work to employees. It is necessary for the regulations' internal consistency, to simplify implementation at this time by reducing the number of notices a business must provide, and to provide further clarity and guidance for businesses regarding how they can consolidate Pre-use Notices.

Non-substantial changes: The Agency has renumbered subsections, made non-substantial grammatical changes (replacing semicolons with periods, updating cross-references) and other non-substantial changes (using "ADMT" instead of "automated decisionmaking technology," and replacing one instance of "student's work" with "students' work").

Amend § 7221. Requests to Opt-Out of ADMT.

Subsection (a): The Agency modified this subsection add the phrase "that uses ADMT to make a significant decision concerning a consumer," to clarify that a business must provide consumers with the ability to out of that use, subject to the exceptions in subsection (b). This is necessary to align with the modifications the Agency made to section 7200, subsection (a), which specifically address the use of ADMT to make a significant decision, as well as to provide clarity and guidance for businesses about when they must provide consumers with the ability to opt-out of their use of ADMT, and to simplify implementation at this time by reducing the

ADMT uses for which businesses must provide consumers with the ability to opt-out.

Subsection (b): The Agency modified this subsection to clarify that a business that uses ADMT to make a significant decision is not required to provide consumers with the ability to out of that use, subject to the exceptions in subsections (b)(1)–(3). This is necessary to align with the modifications the Agency made to section 7200, subsection (a), and section 7221, subsection (a), which now focus on the use of ADMT to make a significant decision, to provide clarity and guidance for businesses about when they are not required to provide consumers with the ability to opt-out of their use of ADMT.

Previous subsection (b)(1): The Agency deleted this subsection as unnecessary in light of the other modifications the Agency has made to the regulations. The other modifications include revisions to the definition of ADMT, which now addresses a higher-risk use of ADMT without human involvement, and modifications to section 7200, subsection (a), to clarify that only a business that uses ADMT for a significant decision concerning a consumer must comply with the requirements of Article 11. In modifying this subsection, the Agency considered the likelihood of a business using technology without human involvement to make a significant decision concerning a consumer. The Agency determined that the human-appeal exception and the fact that a business may deny a consumer's opt-out request if the business believes the request is fraudulent, balance protections for consumers' privacy and preserving businesses' ability to protect themselves and consumers at this time. (*See* subsections (b)(2) and (g).) This modification is necessary to align with other modifications the Agency has made to the regulations, and to provide clarity for businesses about when they are not required to provide consumers with the ability to opt-out of the businesses' use of ADMT.

Subsection (b)(1), previously subsection (b)(2)**:** The Agency modified this subsection to clarify what a business must do to qualify for the human appeal exception and make it easier to read. This includes deleting the word "qualified," because subsection (b)(1)(A) now includes the relevant qualifications of the human reviewer. These modifications are necessary to provide clarity to businesses on how to incorporate human review into their use of ADMT for significant decisions and to give businesses flexibility regarding how to address consumers' concerns about businesses' use of ADMT to make significant decisions about them.

Subsection (b)(1)(A), previously subsection (b)(2)(A)**:** The Agency modified this subsection to provide additional clarity and guidance for businesses regarding what a human reviewer must know, do, and have the authority to do. Specifically, the Agency has clarified that the business must designate a human reviewer to review and analyze the output of the ADMT and any other information that is relevant to change the significant decision at issue, that the reviewer must know how to interpret and use the output of the ADMT that made the significant decision being appealed, and have the authority to change the decision based on their analysis. The Agency also clarified that the consumer-provided information that the human reviewer must consider is information in support of the consumer's appeal. These modifications are necessary to ensure that higher-risk uses of ADMT that lack adequate human review cannot leverage this exception. They also provide clarity to businesses on how to incorporate human review into their use of ADMT for significant decisions concerning consumers, and give businesses flexibility regarding how to address consumers' concerns about businesses' use of ADMT to make significant decisions about them, when offering an appeals process.

Subsection (b)(1)(B), previously subsection (b)(2)(B)**:** The Agency modified this subsection to clarify that the business must enable the consumer to submit information in support of their appeal to the human reviewer, and to clarify when a business must comply with the verification requirements in Article 5. These modifications are necessary to provide clarity and guidance to businesses on how to incorporate human review into their use of ADMT for significant decisions concerning consumers, and to give businesses flexibility regarding how to address consumers' concerns about businesses' use of ADMT to make significant decisions about them.

Subsections (b)(2)(A) and **(b)(3)(A)**, previously subsections (b)(3)(A) and (b)(4)(A)**:** The Agency modified these subsections to remove the requirement that the business's use of ADMT be necessary to achieve the purposes set forth in subsection (b)(2)(A) and (b)(3)(A), respectively. These modifications are necessary to simplify implementation for businesses at this time by making it easier for them to qualify for this exception to providing consumers with an opt-out of ADMT.

Subsections (b)(2)(B) and **(b)(3)(B)**, previously subsections (b)(3)(A) and (b)(4)(A)**:** The Agency modified these subsections to add "unlawfully" and replace "protected classes" with "protected characteristics" for clarity, consistency, and harmonization with existing law and within the regulations.

Subsections (b)(2)(B) and **(b)(3)(B),** previously subsections (b)(3)(B) and (b)(4)(B)**:** The Agency modified these subsection to replace the previous requirements — that the business must have evaluated the ADMT to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes; and implemented policies, procedures, and training to ensure the same — with the requirement that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. These modifications provide a flexible standard applicable to many factual situations and across industries, and are necessary to balance privacy protections for consumers while simplifying implementation for businesses at this time by streamlining the steps required to qualify for this exception.

Previous subsections (b)(3)(B)(i) and (b)(4)(B)(i): The Agency deleted these subsections to align with the modifications to subsections (b)(2)(B) and (b)(3)(B) and to simplify implementation for businesses at this time. This is necessary to simplify implementation for businesses at this time by streamlining the steps required to qualify for this exception.

Previous subsections (b)(5) and (6): The Agency deleted these subsections to align with the modifications the Agency made to section 7200, subsection (a), which no longer include separate thresholds for work or educational profiling, profiling for behavioral advertising, or training uses of ADMT. This is necessary to simplify implementation at this time and keep the regulations internally consistent.

Subsection (c)(1): The Agency modified this subsection to remove the requirement that the link be titled "Opt-out of Automated Decisionmaking Technology" and to replace it with a requirement that the link "state what the consumer is opting out of," with "Opt-out of Automated Decisionmaking Technology" being an example. This modification is necessary to provide businesses with more flexibility and simplifies implementation of the regulations for businesses at this time.

Subsection (n)(1): The Agency modified this subsection to delete the following sentence as unnecessary: "For personal information previously processed by that automated decisionmaking technology, the business must neither use nor retain that information." A business that ceases to process a consumer's personal information using that ADMT already cannot use nor retain that information. This modification is necessary to make the regulations easier to read.

Subsection (n)(2): The Agency modified this subsection to add the word "that" in two places, to clarify which ADMT the consumer has made a request to opt-out of, and therefore which ADMT the business must notify all other persons to whom it disclosed information using that ADMT, that the consumer has opted out, and instruct them to comply with that opt-out within the same time frame. This is necessary because a consumer may have opted out of only certain of the business's uses of ADMT, in accordance with subsection (i). These modifications are necessary to further clarify businesses' obligations with respect to consumers' requests to opt-out of ADMT that have been submitted after the business initiated the processing.

Non-substantial changes: The Agency also renumbered the subsections and made non-substantial changes (for example, using "ADMT" instead of "automated decisionmaking technology," updating cross-references, adding the word "subsections," and deleting unnecessary words such as "of these regulations").

Amend § 7222. Requests to Access ADMT.

Subsection (a): The Agency modified this subsection to align with the modifications the Agency made to section 7200, subsection (a), which now focuses on the use of ADMT to make a significant decision. This is necessary to provide further clarity and guidance for businesses regarding when they must provide information in response to a consumer's request to access ADMT. This is necessary for the regulations' internal consistency, and to simplify implementation at this time by reducing the ADMT uses for which businesses must provide consumers with the ability to access ADMT.

Previous subsection (a)(1): The Agency deleted this subsection to align with the modifications the Agency made to section 7200, subsection (a), which no longer contains a separate threshold for training uses of ADMT. This modification is necessary for the regulations' internal consistency.

Subsection (b): The Agency modified this subsection to clarify what a business needs to provide to a consumer in response to the consumer's request to access ADMT. These modifications are necessary to implement CCPA's direction that businesses provide meaningful information about the logic involved in the ADMT's decisionmaking process, as well as a description of the likely outcome of the process with respect to the consumer. They are also necessary to ensure that consumers have meaningful control over their personal information, including

having sufficient information to determine whether to exercise other CCPA rights, such as the right to correct.

Subsection (b)(2): The Agency modified this subsection to provide a flexible, performance-based standard for businesses regarding how to provide the required information. The Agency has clarified that a business must include information about the logic of the ADMT that must enable a consumer to understand how the ADMT processed their personal information to generate an output with respect to them. The Agency also modified the subsection to add that this information may include the parameters that generated the output, as well as the specific output with respect to the consumer. These modifications are necessary to provide further clarity and guidance for businesses regarding what information they must provide to consumers, so consumers have meaningful information to understand the logic of the decisionmaking process.

Subsection (b)(3), previously subsection (b)(3)(A)**:** The Agency modified this subsection to add that the business must include the outcome of the decisionmaking process for the consumer, including how the business used the output of the ADMT to make a significant decision regarding the consumer. The Agency also added an example of how a business could explain how it used the output of the ADMT to make a significant decision with respect to a consumer, noting that the explanation may include whether the output was the sole factor, or what the other factors were in the business's decisionmaking process, and a human's role in the decisionmaking process, if any. These modifications are necessary to provide further guidance for businesses regarding what they must include in response to a consumer's request to access ADMT and ensure that businesses provide consumers with the most meaningful pieces of information necessary for them to understand how a business used ADMT to make a significant decision with respect to them.

Subsection (b)(3)(A), previously subsection (b)(3)(A)(i)**:** The Agency modified this subsection to add that this information may include whether the output will be the sole factor or what the other factors will be in the business's decisionmaking process, and a human's role in the decisionmaking process, if any. These modifications are necessary to provide further clarity for businesses regarding what they must include in response to a consumer's request to access ADMT if they plan to use the output for additional significant decisions.

Previous subsections (b)(3)(B) and **(b)(4):** The Agency deleted this subsection to align with the modifications the Agency made to section 7200, subsection (a), which now focuses on the use of ADMT for significant decisions, and its deletion of the security, fraud prevention, and safety exception in section 7221, subsection (b)(1). These modifications are necessary for the regulations' internal consistency and to simplify implementation at this time

Previous subsections (b)(4)(A)–(B): The Agency deleted these subsections because the Agency incorporated portions of them into subsection (b)(3). The Agency deleted the remaining requirements from these subsections to simplify implementation for businesses at this time by reducing the amount and granularity of information they must provide.

Previous subsection (b)(4)(C): The Agency moved this to subsection (*l*).

Subsection (c): The Agency added this subsection to clarify that a business is not required to include trade secrets or certain information related to security, fraud prevention, or safety when providing the information required by subsections (b)(2)-(3). This is necessary to provide further clarity for businesses regarding what information they must disclose to consumers, and give businesses flexibility regarding how they can comply with requests to access ADMT, while providing appropriate protections from public disclosure for trade secrets or certain security, fraud prevention, and safety information. These modifications also address public comments that requested protections for trade secret information.

Subsection (e), previously subsection (d)**:** The Agency modified this subsection to make the regulations easier to read and understand. Specifically, the Agency modified the subsection to add the phrase "comply with the verification requirements set forth in Article 5 for requests to access ADMT." This modification is consistent with the modification the Agency made to section 7221, subsection (b)(1)(B). It is necessary to provide clarity for businesses regarding how to comply with consumers' requests to access ADMT, and for the regulations' internal consistency.

Subsection (j), previously subsection (i)**:** The Agency modified this subsection to remove the words "key" and "generally" from the example in the subsection, as unnecessary. The Agency also deleted the reference to subsection (b)(4) to align with the Agency's deletion of subsection (b)(4). This modification is necessary for the regulations' internal consistency.

Subsection (*l*), previously (b)(4)(C)**:** The Agency added the first sentence to clarify that businesses may provide additional information in response to a consumer's access ADMT request. The Agency also moved the example from previous subsection (b)(4)(C) to this subsection. These modifications are necessary to provide further clarity and guidance that a business may provide more information to consumers beyond what is required in subsection (b).

Previous subsection (k): The Agency deleted this subsection to simplify implementation at this time by reducing the number of notices that businesses are required to provide to consumers. Consumers will still receive disclosures regarding the use of ADMT and their CCPA rights via the Pre-use Notice.

Non-substantial changes: The Agency also renumbered subsections and made non-substantial changes (for example, using "ADMT" instead of "automated decisionmaking technology," and deleting "of these regulations" as unnecessary).

ARTICLE 12. INSURANCE COMPANIES

Amend § 7271. General Application of the CCPA to Insurance Companies.

Subsection (b): The Agency modified this subsection by deleting "and requirements." This is necessary to clarify that the examples listed are fact-specific and examples of compliance, not requirements of how an insurance company must comply in every circumstance.

Subsection (b)(3): The Agency modified this subsection to add a third example to clarify how information subject to the Insurance Code would not be subject to the CCPA. This is necessary to address public comments seeking clarification on situations in which the information maintained by an insurance company would not be subject to the CCPA.

UDPATE TO ECONOMIC AND FISCAL IMPACT STATEMENT

Business Impact and Estimated Costs to Businesses

The 15-day modifications to the regulations significantly reduced the direct costs to businesses as summarized below. The cost savings were a result of a decrease in businesses subject to some of the regulations, a reduction of certain requirements and the amount of hours the Agency estimates it will take for businesses to comply,

and an adjustment to a baseline assumption related to cybersecurity audits. The costs savings are explained in greater detail below.

Cybersecurity Audits: The Agency made several changes to the regulations that would lessen the number of hours it would take to conduct an audit. For example, the Agency removed the requirement that, where an auditor deems a component of a cybersecurity program not applicable to a business's information, the cybersecurity audit report document and explain why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security. The Agency also removed the requirement that the business specifically explain how a cybersecurity audit, assessment, or evaluation that it has completed for another purpose meets all of the requirements set forth in Article 9, as well as the requirement that the business provide the cybersecurity audit report to the business's board of directors. Accordingly, based on the Agency's knowledge and expertise, the Agency estimated that the number of hours it would take to audit a business's cybersecurity program would likely decrease by 25%.

The Agency also adjusted its calculation of the cost of an audit to reflect that existing law, including the CCPA, already requires businesses to implement reasonable security procedures and practices. (*See* Civ. Code § 1798.100(e).) All businesses should already be using an existing cybersecurity framework to comply with these existing requirements. Accordingly, the 30% reduction in number of hours to conduct a cybersecurity audit for businesses utilizing an existing cybersecurity framework should have been part of the baseline, and thus, applied to all businesses subject to these regulations.

Finally, there was a change in timing of direct costs for cybersecurity audits because of the modification to phase-in the cybersecurity audit requirements over the course of three years. This spread out the costs of complying with the regulations and provided more time for these businesses to come into compliance.

Risk Assessments: Removing behavioral advertising as a business practice requiring a business to conduct a risk assessment reduced the number of firms the Agency estimates are subject to risk assessment requirements by 2%. The Agency also estimates that the number of hours it would take to conduct a risk assessment decreased by 10% based on Agency's knowledge and expertise. This is because the Agency removed some items that must be included in a risk assessment, including various identification and documentation requirements, such as those regarding the

quality of personal information, the technology used in the processing, criteria used to make determinations regarding negative impacts, identification regarding how safeguards address specific negative impacts, and certain accuracy and nondiscrimination safeguards regarding ADMT. The Agency also removed certain disclosure requirements for businesses training ADMT or artificial intelligence and reduced the granularity of risk assessment information that must be submitted to the Agency, both of which further reduce the time and resources businesses must use to comply with the risk assessment requirements.

Automated Decisionmaking Technology: Modifying the definition of ADMT to focus on technology that replaces or substantially replaces human decisionmaking, and requiring businesses to comply with ADMT requirements only when they use ADMT to make a significant decision concerning a consumer significantly reduced the number of businesses the Agency estimates are subject to the rules. Under the modified ADMT regulations, the Agency estimates that 10% of businesses (5,233 firms) will be required to comply with the ADMT rules. This estimate is based on the Agency's knowledge and expertise regarding how businesses use ADMT to make decisions.

Other sections: The removal of subsections 7022(g)(5), 7023(f)(6), 7024(e), 7026(e), 7027(f), and 7023(f)(3) reduced the direct costs to businesses by over $51.6 million.

Cumulatively, and based on reasonable assumptions and existing data available, the total direct costs over 10 years decreased from $9.725 billion to $4.835 billion. The charts below summarize the breakdown in costs. The large majority of costs (71%) come from the cybersecurity audit regulations, which the statute requires to be annual. Costs attributed to risk assessments, ADMT, and updates to the regulations follow.

	Total 10 Year Costs	*% of Costs*
CSA	$3,437,726,967	71%
RA	$621,222,330	13%
ADMT	$447,719,705	9%
UPDATES	$327,950,540	7%
TOTAL:	**$4,834,619,542**	**100%**

The small business initial costs range changed from $7,045 - $92,896 to $6,058 - $36,950; and small businesses ongoing costs changed from $19,317 to $15,831. Typical business initial costs range changed from $7,045 - $122,666 to $6,058 - $63,133; and typical businesses ongoing costs changed from $26,015 to $19,750.

Estimated Benefits of Regulation

The Agency believes that the 15-day modifications to the regulations delay some of the quantifiable benefits resulting from the regulations. Specifically, the Agency assumes that the phasing-in of cybersecurity audit requirements will delay the corresponding reduction in cybercrimes by a few years. Accordingly, the Agency estimates that the benefits in the first year decreases from $1.5 billion to $1.0 billion.

However, given the cumulative and ongoing reduction in cybercrimes after full implementation of the cybersecurity audit and risk assessment requirements, the Agency believes that the benefits will continue to grow. By the 10th year, the benefits are estimated to increase from the Agency's previous assessment of $66.3 billion to $111 billion. Over 10 years, the benefits will be $282 billion instead of an initial assessment of $186 billion.

There continue to be many other benefits for businesses, individuals and the economy that cannot be quantified at this time. These include things like increased transparency and consumer control over personal information; reduced incidences of unauthorized actions related to personal information and their associated harm to consumers that are not accounted for in the FBI's IC3 Report on cybercrimes; and efficiencies, operational improvements, and competitive advantage for businesses.

Results of the Economic Impact Assessment

The following chart summarizes the 10-year breakdown of total costs and benefits of the regulations, as modified. Notably, the net benefits to California businesses are positive one year after implementation in 2029 and total over $277 billion over a 10-year period. And this is only considering quantifiable benefits resulting from avoided business cybersecurity financial losses, which are attributed to only the cybersecurity audit and risk assessment regulations. As explained in the SRIA, there are many other benefits that cannot be quantified at this time. Also, costs to businesses rapidly decline by 52% in Year 2 and down 81% by Year 10.

(Fig. $2022 B)	Year 1 2028	Year 2 2029	Year 3 2030	Year 4 2031	Year 5 2032	Year 6 2033	Year 7 2034	Year 8 2035	Year 9 2036	Year 10 2037	Total	Avg
COSTS												
Modified	1.28	0.61	0.61	0.42	0.39	0.36	0.33	0.30	0.27	0.25	***$4.8***	***$0.5***
BENEFITS												
Modified	1.00	2.02	3.74	5.96	9.56	15.43	25.05	40.91	67.19	110.97	***$282***	***$28***
NET BENEFITS												
Modified	-0.28	1.41	3.12	5.54	9.17	15.07	24.72	40.61	66.92	110.72	***$277***	***$27.7***

Because the phased implementation of cybersecurity audits is complete by 2030, the impact to the gross state product is positive by 2033 and significantly higher at $375 billion by the 10th year (previously assessed at $290 billion). The Agency anticipates that the modifications to the regulations will change its original estimate for number of jobs created in Year 10 from 233,000 to 358,000. They will also decrease the estimate of jobs eliminated in the first year by 6,000, from 98,000 to 92,000.

LOCAL MANDATE DETERMINATION

The regulations do not impose a mandate on local agencies or school districts.

DOCUMENTS INCORPORATED BY REFERENCE

There are no documents incorporated by reference.

SUMMARY OF COMMENTS AND AGENCY RESPONSES

Please see Appendix A.

ALTERNATIVES THAT WOULD LESSEN ADVERSE ECONOMIC IMPACT ON SMALL BUSINESSES

No alternative proposed to the Agency that would lessen any adverse economic impact on small businesses and be as effective as the regulations was rejected by the Agency.

ALTERNATIVES DETERMINATIONS

In accordance with Government Code section 11346.9, subdivision (a)(4), as discussed in the summary of comments and Agency responses, the Agency determined that no alternative it considered or that has otherwise been identified

and brought to its attention would be more effective in carrying out the purpose for which the action is proposed, as effective and less burdensome to affected private persons than the proposed action, or more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

The provisions adopted by the Agency are the only ones identified by the Agency that will accomplish the goals of effectively updating existing CCPA regulations; clarifying when insurance companies must comply with the CCPA; operationalizing requirements to complete an annual cybersecurity audit; operationalizing requirements to conduct a risk assessment; and operationalizing consumers' rights to access ADMT and opt-out of ADMT. The regulations provide clarity and guidance for businesses and balance protections for consumers' privacy and flexibility for businesses in meeting their compliance obligations.

NON-DUPLICATION

Two sections of the regulations repeat or rephrase in whole or in part a state or federal statute or regulation. This was necessary to satisfy the clarity standard set forth in Government Code section 11349.1, subdivision (a)(3).

First, in section 7001, subsection (bbb), the Agency modified the definition of "sensitive personal information" to add a consumer's neural data. This reflects the updated statutory definition of this term, and improves clarity and readability in the regulations by having the relevant statutory definition available in section 7001.

Second, in section 7154, the Agency modified the section to state the goal of a risk assessment, which is stated in the CCPA. This improves clarity and readability in the regulations by having the goal of the risk assessment in the same place as the relevant risk assessment requirements.